SAPIENZA
UNIVERSITÀ DI ROMA

BlueTracer:
a Robust API Tracer for Evasive Malware

Faculty of Information Engineering, Informatics and Statistics

Master of Science in Engineering in Computer Science

Candidate

Simone Nicchi
ID number 1705157

Thesis Advisor

Prof. Camil Demetrescu

Co-Advisors

Dr. Daniele Cono D'Elia
Dr. Emilio Coppa

Academic Year 2017/2018

BlueTracer: a Robust API Tracer for Evasive Malware
Master thesis. Sapienza – University of Rome

This thesis has been typeset by LaTeX and the Sapthesis class.

Author's email: nicchi.1705157@studenti.uniroma1.it

Ai miei genitori, che non hanno mai smesso di supportarmi

Abstract

As a multitude of new malware instances arise every day, dynamic analysis techniques have assumed a key role in the detection and inspection of malicious software. One of the most adopted dynamic analysis strategies is function call monitoring, since the abstractions embodied by API calls and system calls can be used to comprehend the visible behaviour of the malware sample under analysis, regardless of any obfuscations made on its code. Function call monitoring is typically implemented by means of API hooking, i.e., the interception of function calls made available by dynamically linked libraries (DLL). However, all dynamic analyses techniques - including API hooking - have to face the adversarial behaviour of *evasive malware* strains, which check if they are being executed in a hostile environment and conceal their malicious behaviour accordingly. Furthermore, the majority of API hooking techniques proposed to date in literature are easily detectable by malware and are not equipped with any cloaking method to hide their presence from evasive malware.

We propose a robust library and system call tracer for Windows applications, specialized in evasive malware. To implement our tool, we used the Intel Pin dynamic instrumentation framework, which allows to transparently inject analysis code in a running binary program. In addition, our tool was integrated with BluePill, a stealthy execution framework developed at Sapienza University and Royal Holloway university, enabling it to counteract a wide range of evasive techniques. Our tracer is capable of tracing input parameters, output buffers and return values of a plethora of system calls (including Windows Native APIs) and library calls, as well as the occurrence of user-mode callbacks and Windows Asynchronous Procedure Call. We first evaluated our tool on a set of benign applications performing a variety of tasks and exercising a large number of functions. Then, we validated it through the use of a popular security product aimed at assessing a how stealthy a malware analysis system is with respect to a large portion of public evasion techniques employed by real malware families.

Contents

Chapter 1

Introduction

The term malicious software (*malware* for short) describes any software specifically designed to bring harm to a computer system. Accurate and efficient analysis of malware is a compelling problem that is becoming increasingly important as hundreds of new malware strains arise every day in an ever-growing trend, while the economical damage for organizations keeps worsening [11].

To face this threat, professionals are typically aided by a range of automatic tools capable of analyzing and detecting malicious software. In particular, malware analysis can be carried out either statically or dynamically. Static analysis involves the inspection of the different code and data sections of a binary, but is often frustrated by obfuscation mechanisms and other countermeasures employed by malware authors. Dynamic analysis techniques dodge the problem by executing a malware sample and observing the actions it performs on the environment, and are better suited for dealing with large quantities of samples; these two factors have strongly favored the adoption of dynamic analyses in the security practice.

One of the most employed dynamic analysis techniques is function call monitoring. Generally speaking, a function is made up of code that carries out a particular task, such as creating a file or printing a message. A property that makes functions particularly valuable from a program analysis perspective is that they can abstract implementation details - especially in the case of library and system calls - providing a semantically richer representation of some functionality. Consider for instance a sorting function: details of the underlying algorithm might not be important as

long as one knows that the function sorts an input list. In the context of dynamic analysis, the abstractions embodied by API calls and system calls are incredibly helpful since they can be used to grasp the visible behavior of the sample under analysis, regardless of any obfuscations made on its code.

The most popular technique used for function call monitoring in dynamic malware analysis is API hooking, i.e., the interception of function calls provided by dynamically linked libraries (DLL). The idea is to alter execution so that for each call in the sample, besides the function of interest, a hooking function is called, too. Such function is in charge of performing the desired analysis, which may require for instance logging the invocation on a file or analyzing its parameters.

A problem that nearly all dynamic analyses - including API hooking - have to face is adversarial behavior from *evasive malware*, i.e., malware that actively checks whether it is being executed in a hostile environment, such as a well-known sandbox solution for dynamic analysis. In that case, an evasive sample conceals its harmful behavior to avoid detection, for instance by executing an exit sequence. Evasive techniques are frequently adopted by modern malware. According to a March 2018 Symantec Internet Security Report, 18% of recently observed new samples are aware of hardware virtualization solutions used also for malware analysis [20]. To make matters worse, most API hooking techniques proposed to date in literature are easily detectable by malware, and not coupled with mechanisms to hide their presence from evasive malware.

Contributions. The core contribution of my thesis is the design and implementation of BlueTracer, a robust library and system call tracer for Windows programs specialized in evasive malware.

BlueTracer is based on the Intel Pin [22] dynamic binary instrumentation framework, which allows for transparently injecting analysis code in a binary program as it executes. BlueTracer can effectively counteract a large variety of evasive techniques due to its integration with BluePill [12], a stealthy execution framework being developed at Sapienza University and Royal Holloway University of London that allows the simulation of the original execution environment a particular malware

sample was designed for, and conceals any analysis artifacts or setup details that might set off evasion [12].

BlueTracer can trace input parameters, output buffers and return values of an extremely wide range of system calls (including Windows Native APIs that are invoked directly via special CPU instructions in more advanced malware) and library calls. Moreover, it also supports the tracing of user-mode callbacks and Windows Asynchronous Procedure Calls.

The heterogeneity of Windows libraries used in malware and the lack of well-structured documentation for their prototypes and input/output parameters posed a significant implementation challenge, which BlueTracer addresses by leveling out and integrating reliable external sources (two industry projects: Dr. Memory and CISCO PyREBox) that account for more than 17,000 existing function prototypes. An important engineering effort was also required to make best use of Intel Pin's capabilities with respect to run-time CPU and memory costs, as well as to address some inherent limitations that emerged on the field.

We first validated BlueTracer on benign applications exercising a large number of functions, and then on a popular security product used for assessing how stealthy a malware analysis system is against a large body of public evasion techniques used in the wild. The obtained results suggested that BlueTracer can be very effective in tracing a malware sample's activities while remaining undetected.

Structure of the Thesis. The remaining part of this thesis is structured as follows. Chapter 1 describes the major *API hooking* techniques present in literature, outlining their stengths and weaknesses, especially from a detection point of view. It also introduces the concept of Dynamic Binary Instrumentation (DBI), which constitutes BlueTracer's core. Chapter 3 focuses on the implementation of the tool, on its structure and the design choices which were made during its development. Chapter 4 illustrates the experimental results and assesses the tool's effectiveness. Finally, we present concluding remarks in Chapter 5, together with possible future developments.

Chapter 2

Background

In literature there are many different implementations of API hooking. The objective of this chapter is to provide an outline of the various approaches utilized to hook functions in DLLs, outlining the benefits and the limitations of each technique, with a strong focus on their detection by malicious software. In particular, the focus will be on user space API hooking of `Win32` binaries, since this is BlueTracer's current field of application. Obviously, as it is the norm in malware analysis, it also assumed that the program under study is only available in binary form.

Depending on their underlying implementation, API hooking techniques can be divided in three broad categories: **Binary Rewriting**, **Virtul Machine Introspection (VMI)** and **Dynamic Binary Instrumentation (DBI)**.

2.1 Binary Rewriting

Binary rewriting-based hooking involves inserting hooks at the API entries, via one of the following two approaches:

1. Redirecting all `call` instructions so that the hook is called instead of the original function.

2. Rewriting the function of interest such that, before its invocation, the hook is executed.

In both cases the hook function gains access to all the arguments present on the stack, thus being able to carry out all the required analysis operations.

The main techniques which use the first approach are *Import Address Table (IAT) Patching*, *Export Address Table (EAT) patching* and *Proxy DLL*. On the other hand, the most significant techniques which use the second approach are *inline hooking* and *debugger-based hooking* (*Figure 1.1*).

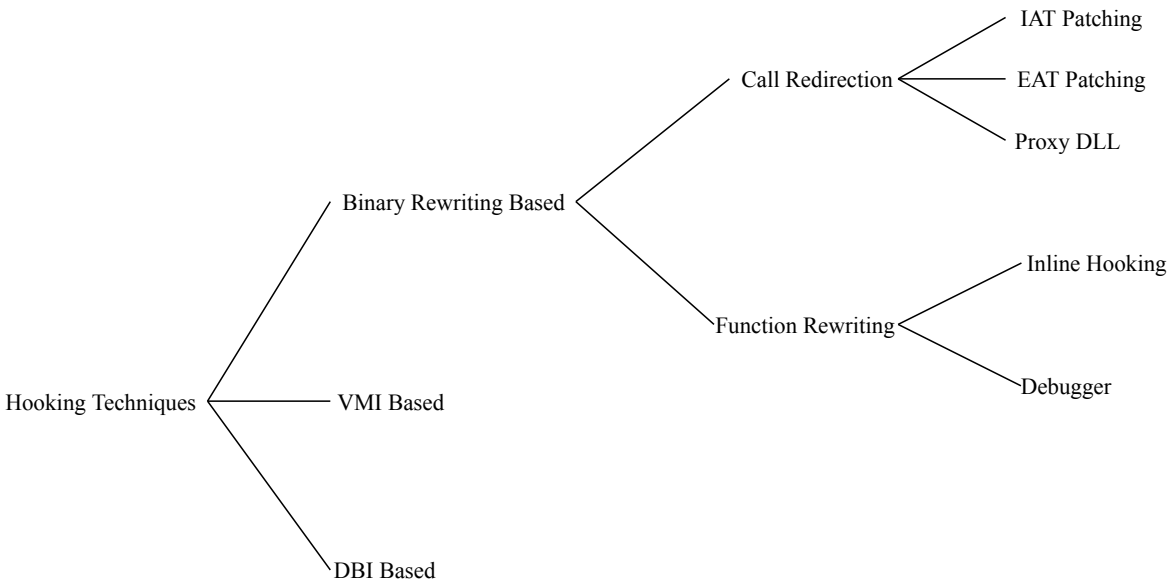

Figure 2.1. *API hooking techniques classification*

2.1.1 Import Address Table Patching

In the header of every Portable Executable (PE) file there is an Import Address Table (IAT) for every dynamic-link library (DLL) that is included by the executable [6] (*Figure 1.3*). This table is utilized to indicate the location of DLL-imported functions in virtual memory and is filled by the Windows loader with the actual function memory addresses after the executable is loaded in memory.

The idea is to overwrite the original pointer to an imported API function so that, instead of pointing to the original API, it will point to a different function.

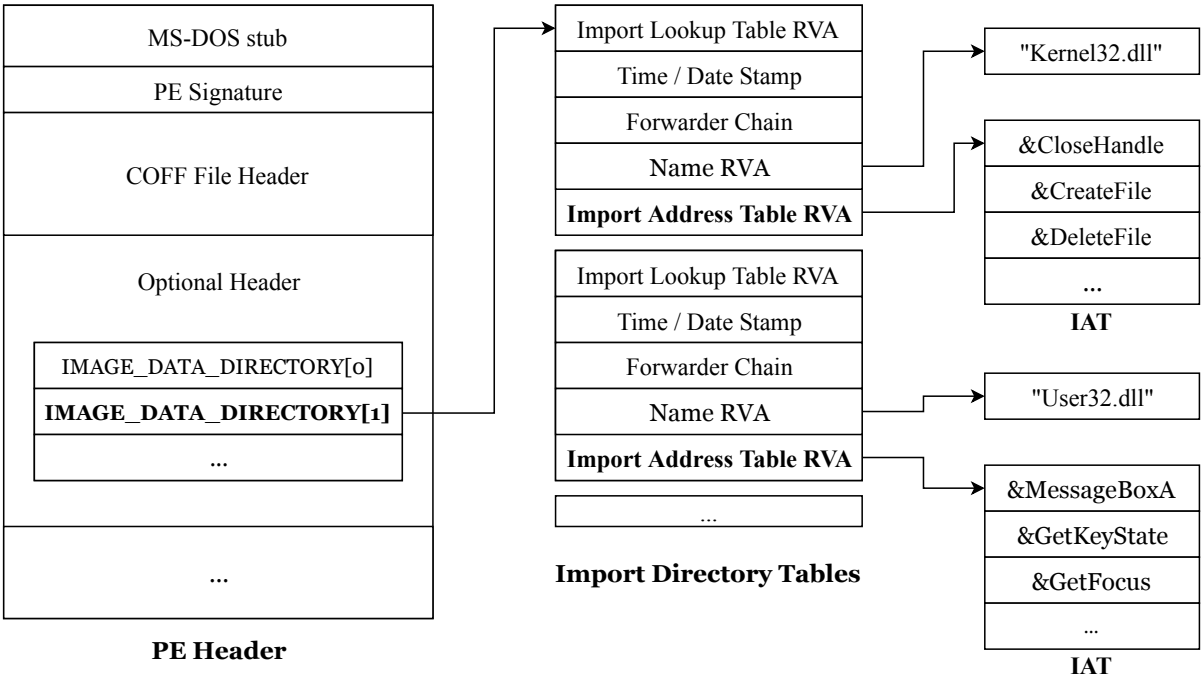

Figure 2.2. *IAT in PE header*

Despite being extremely simple to implement, IAT patching suffers from a couple of disadvantages, which significantly limit its use in practice:

- It is incredibly easy to detect by simply examining the entries of the IAT and checking whether or not each address falls inside the memory range of the DLL that should contain the function [25].
- It is ineffective when function pointers are acquired dynamically, e.g. via `LoadLibrary` and `GetProcAddress` [7].

2.1.2 Export Address Table Patching

Export Address Table (EAT) patching is similar to IAT patching, with the difference that DLL export address tables are patched instead. The export address table (EAT) contains the name of every function exported by the DLL together with the relative virtual address (RVA) where the function can be found, which is relative to the DLL base address when loaded in memory. To hook an API function via EAT patching all that is needed is to overwrite the corresponding address in the table with the address of another function.

EAT patching produces similar results to the ones obtained through IAT patching, but, unlike IAT patching, the created hooks are global, i.e. they affect every program which utilizes the altered DLL [6].

However, in a similar manner to what occurs for IAT patching, it can be easily detected to by simply examining the entries of the EAT and checking whether or not each RVA, when added to the DLL base address, falls within the DLL memory range [36].

2.1.3 Proxy DLL

In the Proxy DLL approach to hooking, also known as Trojan DLL, the DLL containing the functions to be hooked is replaced with another one having an identical name and exporting all the symbols of the original DLL [21]. In addition to calling the original functions so that they can carry out their tasks, the Proxy DLL may also make available different implementations for the hooked functions [6].

Even though a Proxy DLL is trivial to implement, it is also extremely easy to detect since the original DLL is substituted with another file, which is very likely to have a different size. Moreover, checksums could be employed to detect the presence of a Trojan DLL.

2.1.4 Inline Hooking

In *inline hooking* the API to be hooked has its initial instructions (at least the first 5 bytes) overwritten with an unconditional jump to a replacement function. In order to ensure that the API's original functionality is not lost due to the modification of its entry point, a *trampoline function* is created, consisting of a copy of the overwritten instructions and an unconditional jump back to the unaltered portion of the original function. As a result of this, the replacement function can invoke the original function by calling the trampoline, after performing all the desired analysis operations [6]. *Figure 4* illustrates a program's execution flow before and after the use of *inline hooking*.

Inline Hooking, which was made famous by its employment in the Microsoft *Detours* Windows API hooking library, is one of the most used API hooking techniques

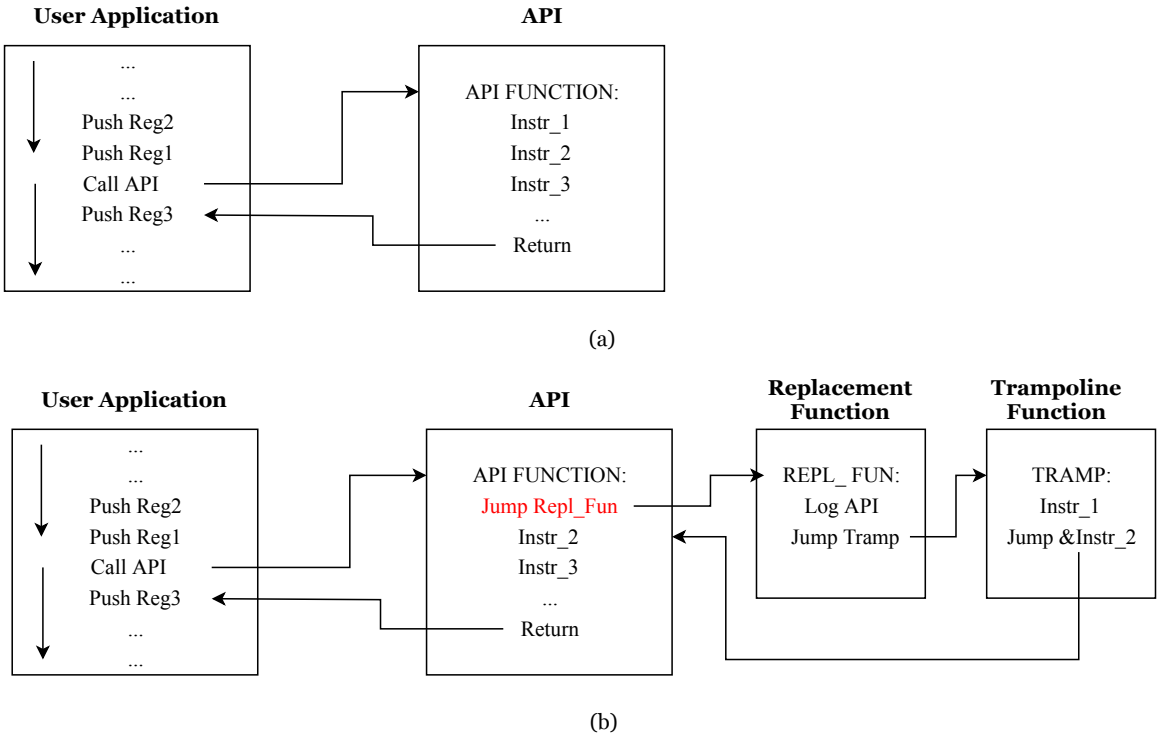

Figure 2.3. *(a) Ordinary API call execution flow*
(b) API call with inline hooking

since it offers a number of advantages:

- It is fast and efficient.
- It can be utilized to hook any code, not just operating systems APIs, but also programmer defined functions [34].
- Unlike IAT patching, the type of command used to call the function does not matter, meaning that the hooking will be effective regardless of the fact that a function is called using the IAT or using `LoadLibrary` together with `GetProcAddress`.

Unfortunately though, *inline hooking* is also affected by some limitations:

- Can be easily detected, for instance by comparing the code section of system libraries in memory with a matching original copy loaded from the file system to detect library modifications [7] or by searching API entry points for specific patterns (e.g. presence of `jmp` instructions) [25].

- It needs additional modifications in the case where the function's entry points includes specific instructions, like ones which contain relative memory addresses. In fact, such instructions cannot be executed from a trampoline as the trampoline is located in a different memory location than the one of the original program code [6].

2.1.5 Debugger-Based Hooking

Hooking through the use of a debugger is realized by instructing the debugger to position a breakpoint at the entry point of the target API function. The placement of a breakpoint involves overwriting the initial instructions of the target API functions with CPU specific instructions, like `INT 3` for `IA-32`. These lead the CPU to throw a debug exception in case they are pointed by the current instruction pointer (IP). The exception is then intercepted by the debugger, which is able to deduce the API which is being called by the application from the address at which the exception took place [25]. Moreover, the debugger also has total control over the memory contents and the CPU state of the process being debugged.

Contrarily to inline hooking, a debugger can be used to hook functions whose entry points include instructions containing relative addresses [6].

On the other hand, a debugger is much easier to detect. In fact, there exist specific Windows APIs whose purpose is to find out whether or not the current process is being debugged. For example, `IsDebuggerPresent` allows to determine if the calling process is running under a debugger, while `CheckRemoteDebuggerPresent` checks for the presence of a debugger in a separate process. In addition, the `INT 3` instruction in an API entry point immediately gives away the debugger's presence [25].

2.2 Virtual Machine Introspection

Hooking based on Virtual Machine Introspection (VMI) relies on the idea of executing the target program in an emulated environment, typically with QEMU being used as virtual machine monitor (VMM). Function calls are monitored by comparing the

virtual processor's instruction pointer with the RVAs of DLLs' exported functions when added to the DLL base address. Function arguments are also monitored and this is done by providing them to callback routines, which perform the appropriate tracking operations.

In theory, a PC emulator allows to have functionalities similar to the ones of a debugger, i.e. the code being monitored can be stopped at any arbitrary point during its execution, allowing its registers and virtual memory to be inspected, with the added advantage of not being subject to the aforementioned issues related to breakpoints. Moreover, VMI-based hooking is harder to detect with respect to the previously illustrated hooking techniques, since emulation is utilized to execute an unknown binary with a complete operating system in software, without the sample being never ran directly on the processor [5].

The significant drawback of VMI-based hooking is that it incurs in the *semantic gap* problem, i.e. the issue of deducing high-level information from the raw system information by making sense of the CPU state and memory contents [18]. VMI-based hooking tools might need an in-depth knowledge of kernel data structures or other details at low-level, which could constitute a complication when dealing with proprietary operating systems. For this reason, as of right now, VMI is not as effective in practice as a traditional debugger when investigating a sample.

2.3 Dynamic Binary Instrumentation

Instrumentation is commonly referred to as the act of adding extra analysis code to a program. There are two main instrumentation techniques being employed in dynamic binary analysis, where the main difference is constituted by when the instrumentation process takes place:

- *Static Binary Instrumentation*, which takes place before the application is executed and involves the rewriting of object code or executable code.
- *Dynamic Binary Instrumentation* (DBI), which happens at run-time. The analysis code can be injected by a specific program attached to the target process or by an external process [26].

Dynamic Binary Instrumentation (DBI) is, therefore, a dynamic binary analysis technique in which the behavior of an application is inspected at run-time via the injection of analysis code. Such code, after being injected, executes as a component of the ordinary instruction flow, allowing to learn information about the behavior and the state of a sample at different points during its execution [15]. Typically, DBI tools make use of a Just In Time (JIT) compiler to instrument the binary under analysis at run-time, the purpose of which is to translate `x86` code into an intermediate representation [28].

DBI, conversely from static binary instrumentation does not need any preprocessing of the program to be analyzed. This is what makes it more appealing for developers for profiling and tracing purposes. On top of that, DBI can be utilized for any program while static techniques are restricted in the code they can instrument, e.g. they cannot employed for code that is dynamically generated [4]. The main drawback of DBI is that the instrumentation cost is encountered at run time, leading to performance degradation. However, in recent years, this issue has been mitigated by the introduction of generic DBI frameworks, which are accurately optimized to minimize the execution overhead [26].

In DBI-based hooking, the idea is to use DBI with the objective of learning information at run-time relative to which APIs are called by the sample being analyzed and, possibly, with which arguments and return values.

There indeed exist DBI-based API tracing tools that rely on the previously illustrated idea, namely *drstrace* and *drltrace*, which are both built on top of the DynamoRIO [16] DBI framework. In particular, *drstrace* is a system call tracer for Windows, while *drltrace* is an API calls tracer for both Windows and Linux applications. They both produce a textual log, in which the invoked APIs are recorded, together with their arguments' values and return values.

In order to evaluate the effectiveness of such tools in the context of evasive malware analysis, a series of experiments involving them was carried out. In particular, both tools were employed to analyze 1000 random samples from the

Arancino[1] dataset of malware samples (about 20% of the total). Each malware sample was ran for 5 minutes in a VirtualBox environment with Windows 7 `x86` SP1 as the guest operating system. The analysis of the resulting logs showed that both tools possess critical shortcomings when analysing evasive malware. In particular:

- They are not equipped with any mechanism aimed at cloaking the execution environment in order to prevent a malicious sample from detecting the DBI.
- They are limited in the amount of information recorded relative to the traced APIs. This applies particularly to *drltace*, which, unlike *drstrace*, does not log return values and output values for arguments, in addition to not providing a mechanism for translating enumerations' constants to the appropriate name. Furthermore, both tools do not take into consideration Windows callbacks and asynchronous procedure calls (APC).

This highlights how the current DBI-based methods are lacking when having to deal with the dynamic analysis of evasive malware and that there is much room for improvement in this area.

2.4 Conclusion

In this chapter we showed how the state of the art API hooking techniques suffer from a number of remarkable shortcomings, especially when dealing with evasive malware. In fact, binary rewriting-based hooking techniques are all easily detectable, while VMI, although harder to uncover, is affected by the *semantic gap problem*. Finally, existing DBI-based API tracing tools are not accompanied by adequate cloaking mechanisms and are limited in the amount of logged information. The aforementioned issues indicate that there is a need for a robust API tracer, specialized in the analysis of evasive malware and with extensive logging capabilities. This is the rationale at the heart of BlueTracer.

[1] Arancino is a dynamic protection framework aimed at providing protection from anti-instrumentation attacks [28]

Chapter 3

Architecture and Implementation

In this chapter we discuss the implementation of BlueTracer, providing a detailed account on how the tool is organized, on the design choices which were made during its development process and on how encountered challenges were dealt with.

3.1 General Overview

We will start the current chapter by giving a general overview of BlueTracer. Specifically we will describe the main characteristics of Intel Pin, the DBI framework on which BlueTracer is based on. Then we will introduce BluePill, the DBI-based software toolkit allowing BlueTracer to be robust against evasive malware. Lastly, we will illustrate BlueTracer's structure, which will serve as a baseline for the rest of the chapter.

3.1.1 Intel Pin

BlueTracer is implemented using Pin, a dynamic binary instrumentation framework by Intel, which is vastly utilized for program analysis, testing of software and in the security field. The version of Pin used for the development of the tool is 3.5, in order to benefit from the notable improvements, both in terms of execution speed and offered features, which were introduced going from the 2.14 release to the 3.x series.

Pin comes with its own OS-agnostic and compiler-agnostic runtime, called PinCRT. PinCRT exposes three layers: a generic operating system interface providing basic OS services (e.g. process and thread control), together with C and C++03 (without RTTI) runtime layers [27].

The most significant features provided by Pin are the following:

- **User-friendliness**. Pin's user model enables the insertion of analysis code in arbitrary locations of the binary through the use of its uncomplicated but rich C and C++ APIs.
- **Portability**. Pin's APIs are independent from the architecture but, at the same time, they allow the extraction of architecture-specific information.
- **Transparency**. The information obtained by Pin perfectly describes the program's original actions. This because an application instrumented by Pin preserves instruction and data addresses as well as memory and register values of the uninstrumented execution.
- **Efficiency**. Pin employs a just-in-time (JIT) in order to add and optimize analysis code. It makes use of a set of optimization techniques, including code caching and inlining.
- **Robustness**. Pin uncovers code at run-time and is thus able to manage dynamically generated code, dynamically loaded libraries and the targets of indirect jumps which are statically unknown.

An analysis tool built using Pin, commonly known as a *pintool*, is made up essentially by two types of routines: analysis routines and instrumentation routines. Analysis routines embody the code to be inserted during the application's execution which is in charge of collecting application-related information. On the other hand, instrumentation routines determine where the analysis code has to be placed.

Moreover, in Pin there exist different granularities with respect to the instrumentation routines, namely image, routine, trace and instruction granularities. A granularity for a instrumentation routine defines when the instrumentation routine

should be invoked. For instance, in the case of instruction granularity, the instrumentation routine is executed for each instruction. In a similar way, Pin also supports analysis-routine granularities, which define where the analysis routines should be placed [4].

3.1.2 BluePill

BlueTracer remains undetected from evasive malware thanks to its integration with BluePill, which essentially constitutes BlueTracer's foundations. The main concept behind BluePill is the idea of using DBI to deceive highly evasive malware instances into believing they are executing in the environment they are designed to attack.

BluePill [12] is a software toolkit built on top of the Intel Pin DBI framework which:

- Allows the simulation of a real production environment a specific malware sample was intended for.
- Conceals any virtualization artifacts and software setup which might set off evasion.

In particular, BluePill implements over 100 Windows anti-evasion techniques as a set of low-level primitives aimed at monitoring, inspecting and faking the outcomes of malware operations investigating the execution environment. Experimental results have validated BluePill's effectiveness and have shown its ability to hinder a wide range of evasion mechanisms.

One of the BluePill's core components is the *Target platform simulation layer*. It is in charge of managing how API calls, system calls and special instructions leak execution environment-specific information to the malware instance. In fact, details like operating system, hardware and the execution environment need to be tailored to meet the sample's expectations. BlueTracer operates at this level. In fact, BlueTracer complements BluePill by providing a detailed account of the malware instance activity, allowing the analysts to understand in detail what the malware's actions are. So, while BluePill's *Target platform simulation layer* is aimed at deceiving the malware sample, BlueTracer tracks the information related to the

malware activity before it is tricked, allowing to determine what the malicious sample was attempting to do. In this way it is possible to track in detail the activity of a malware sample, a feature BluePill lacks, while, at the same time, not worrying about the sample's anti-evasion activity, since this is addressed by BluePill.

In light of what just stated, BlueTracer's integration with BluePill is straightforward, since it essentially complements the *Target platform simulation layer*, as it can be observed from *Figure 3.1*.

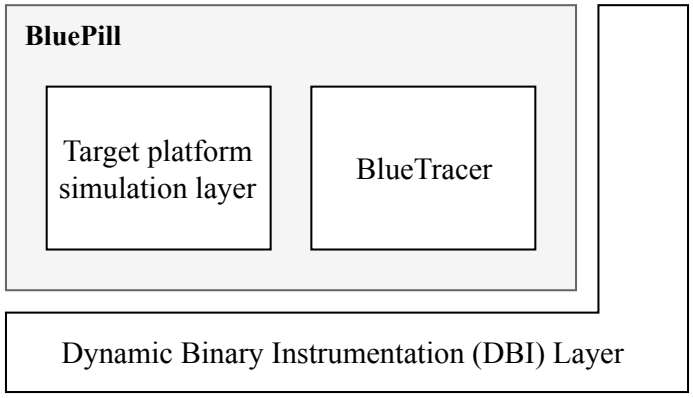

Figure 3.1. *BlueTracer's integration with BluePill*

3.1.3 Structure

BlueTracer has been organized primarily taking into account the rich set of APIs offered by Pin, which have led to the decision to split the tool in three parts: the first aimed at **Native APIs tracing**, the second for **APIs tracing** and the last focused on **callbacks and APCs tracing** (*Figure 3.2*). In particular, the tracing of native APIs also employs a different source of API information (*Dr. Memory*'s system call data) than the ones utilized for tracing APIs (*drltrace*'s configuration file or the information extracted from *PyREbox*'s database).

This chapter will proceed by describing how multi-threading was addressed in the tool, as this is central to all its components. Then, the implementation of each one of three aforementioned parts will be discussed in detail.

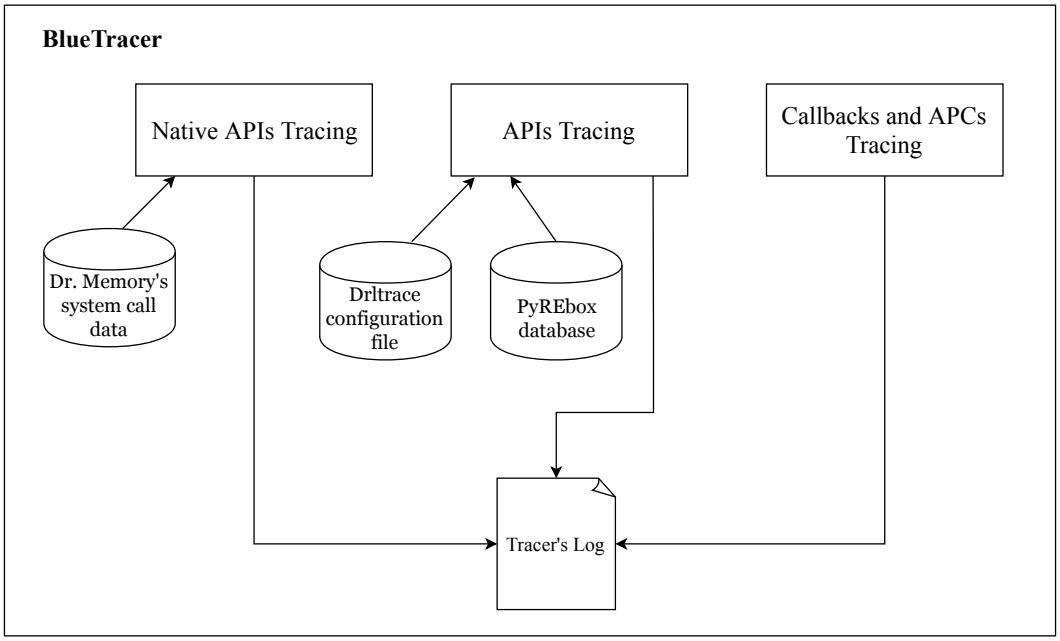

Figure 3.2. *BlueTracer's high level structure*

3.2 Thread Management

Since the samples under analysis are typically multithreaded applications, let us go through the mechanisms exposed by Pin to manage threads and how those were employed in the implementation of the tool.

Pin assigns to each thread an ID, a small number beginning at 0 which is not the same as the operating system thread ID. A way to obtain such ID is by using as analysis routine argument `IARG_THREAD_ID`, which passes the thread ID assigned by Pin for the calling thread. This ID is typically used as an index of an array of thread data. In fact, the Pin API makes available an efficient thread local storage (TLS). In order to utilize it, it is first required to allocate a new TLS key via `PIN_CreateThreadDataKey`, which can optionally take as input a pointer to a destructor function. After that, any thread of the process can use the TLS key, in addition to its Pin-specific thread ID, to store (`PIN_SetThreadData`) and retrieve (`PIN_GetThreadData`) values in its own slot. The starting value relative to the key in every thread is `NULL`. Pin makes also available call-backs when each thread starts (registered with `PIN_AddThreadStartFunction`) and ends (registered with `PIN_AddThreadFiniFunction`). This is typically where thread local data is

allocated, manipulated and stored in a thread's local storage[27].

In BlueTracer, each TLS slot stores a `struct` of the type `bluepill_tls` (*Listing 3.1*) for every thread. Such `struct` is dynamically allocated every time a thread starts in the `OnThreadStart` callback function and is consequently deallocated in the `onThreadFini` function when the thread ends.

```
1  typedef struct {
2   ...
3   syscall_tracer* syscallEntry;      // Pointer to NTAPI entry
4   vector<stackEntry>* shadowStack;  // Shadow stack
5   uint call_number;                 // Calls counter
6
7   buf_info_t* buffer;               // Buffer for writing to file
8   FILE* OutFile;                    // Output file pointer
9
10  // Pointer to function for opening file/writing to file
11  void(*file_write)(THREADID, buf_info_t*, FILE*, const char*,   ...);
12
13  ...
14 } bluepill_tls;
```

Listing 3.1. Thread Local Data

Since the first three fields of the above `struct` (lines 3-5) are employed when tracing native APIs and APIs, they will be discussed in detail later in the chapter. Now let us focus on the remaining fields, which are used by BlueTracer to write the traced information in the appropriate log files.

3.2.1 Log Files and Multithreading

In BlueTracer, the traced data is written to a binary file, one for every thread. The default naming convention used for the tracer's log files is `Traced.[OS Process ID].[Pin-specific Thread ID]`, similarly to the one BluePill employs in its own log files, with the user being able to change `Traced` with a name of its choice in the configuration file.

When writing data to file, each thread invokes the `file_write` function, whose

pointer is located in the instance of the `bluepill_tls` struct associated to the thread (line 11 of *Listing 3.1*). However, such data, which follows the same format of strings used by `fprintf`, is not directly written to file. Instead, an intermediate 8 kB buffer is used (line 7 of *Listing 3.1*): only when the buffer is full (or when the amount of data to be written does not fit the buffer) file writing actually occurs. The choice of using a buffer was made as an attempt to improve performance, as it allows the aggregation of small write operations into a block size that is more efficient for the disk subsystem.

A problem which was encountered when trying to conjugate file management and multithreading is that there exists a known isolation issue affecting Pin on Windows. Specifically, it is possible for a deadlock to take place if a file is opened in a callback in the context of multithreaded applications. As a result of this issue, it is not possible to open the tracer's log file in the `OnThreadStart` callback. Pin's manual proposes to circumvent the problem by opening the file in the `main` and tagging the data with the thread ID [27]. However, this conflicts with the idea of having one file for each thread.

In order to bypass this limitation of the Pin's framework, the following strategy was employed:

1. When initializing the thread local data in `OnThreadStart`, `file_write` is set to point to a function named `file_open`.
2. The first time a thread attempts to write data to file `file_open` is invoked.
3. `file_open` carries out the following actions:
   (a) Opens the tracer's log file (this is safe since the file is not opened in a callback)
   (b) Sets the obtained file pointer in the thread local data (line 8 of *Listing 3.1*)
   (c) Adds the data to be written in the buffer (which is eventually written to file if the buffer is too small to hold it)
   (d) Sets `file_write` to point to `buf_write`, a function which is in charge of just writing data to the buffer and to file.

4. As a result of this, when the thread attempts to write to file again, `buf_write` is invoked, thus allowing the thread to just write to file without going through opening the file again.

3.3 Native APIs Tracing

Windows Native APIs are employed to call operating system services in kernel mode in a controlled way. In fact, all core Windows components, which possess direct access to hardware and services in charge of handling the computer's resources (e.g. memory), operate in kernel mode. This means that, every time a user mode application desires to carry out certain actions, like for instance starting a thread or allocating virtual memory, they must rely on kernel mode services. The Windows Native API corresponds to the system call interface of standard monolithic operating systems, such as the majority of UNIX-like systems, with the difference that in the latter case the system call interface is documented and can be utilized directly by applications. Instead, due to Windows' architecture, Windows Native APIs are concealed to the programmer by the higher level Windows (`Win32`) APIs [31]. User mode Windows Native APIs, which are identified by their `Nt` prefix and are exported by `ntdll`, have caught the attention of malware writers since they are seen as a way of bypassing the documented APIs with the objective of performing a series of actions without being discovered [8]. For this reason it is a good idea to also trace them, in addition to the ordinary Windows APIs.

Pin provides a set of APIs aimed at assisting the extraction of information relative to the system calls made by the pinned application, also including information relative to Windows Native APIs. In particular, in BluePill (and consequently in BlueTracer) `PIN_AddSyscallEntryFunction` and `PIN_AddSyscallExitFunction` were used for this purpose. In fact, these allow to register notification functions which are called immediately before and after the execution of a system call [27]. In BlueTracer, the function in charge of gathering Native API information before execution is `TraceSysCallEntry` while the one responsible for collecting Native API information after execution is `TraceSysCallExit`. They have been both been embedded in BluePill's notification functions and their overall structure is detailed in *Figure 3.3*.

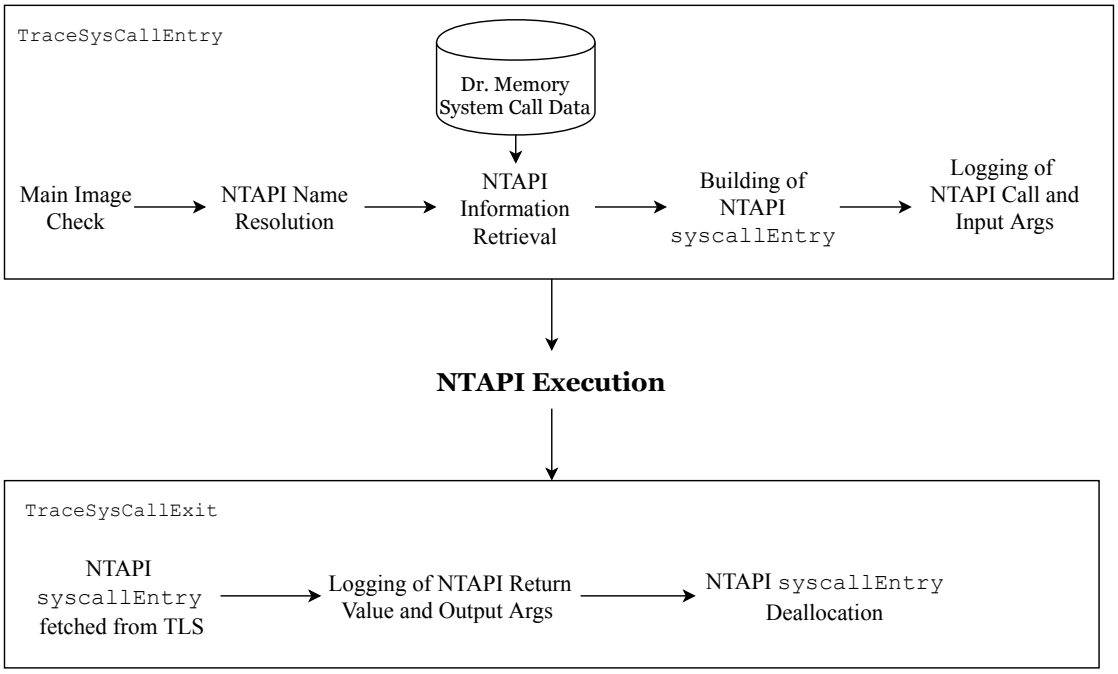

Figure 3.3. *Native APIs Tracing Workflow*

Following *Figure 3.3*, let us now thoroughly analyze the main steps which take place when Native APIs are traced.

3.3.1 Main Image Check

In order to filter the logged information relative to Native APIs, BlueTracer allows the analyst to decide, through the use of a boolean parameter (`MainImage`) in the configuration file, whether or not only Native APIs called invoked directly from the main executable of the pinned application should be traced. Therefore, as it can be seen in *Figure 3.3*, the first thing which is done in `TraceSysCallEntry`, assuming that the `MainImage` configuration parameter has been set to `true`, is to determine if the Native API call is taking place directly from the main executable.

To this end, Pin's `IMG` APIs are employed, where in Pin an `IMG` represents all the data structures relative to binaries and shared libraries [27]. Specifically, in BluePill, `IMG_AddInstrumentFunction` is utilized to register a callback which is invoked each time an image is loaded. Inside such callback, which takes as one of the

input parameters the `IMG` object representing the image being loaded, the following steps are taken:

1. `IMG_IsMainExecutable` is employed to determine if the image being loaded is the main executable of the pinned application.

2. If this is the case, `IMG_HighAddress` and `IMG_LowAddress` are invoked. These two APIs return the highest address and the lowest address respectively of any code or data loaded by the image corresponding the the `IMG` object they take as input. By employing these APIs is therefore possible to determine the address range relative to the main executable.

Having obtained the main executable address range in this way, it is then employed in `TraceSysCallEntry` to learn if the Native API call is occuring directly from the main image. Internally, before entering kernel mode every Native API executes some common code, i.e. each Native API stores its ordinal in the `eax` register and invokes `KiFastSystemCall`, where the `sysenter` instruction is used to actually enter kernel mode. When `sysenter` is executed, the kernel obtains the ordinal number from `eax` and utilizes it to call the corresponding function, prior to going back to user mode [19].

In Pin, the Native API is intercepted right before `sysenter` is executed. This could be inferred by the fact that, in `TraceSysCallEntry`, the instruction pointer (obtainable via the `PIN_GetContextReg` API) contains `sysenter`'s address. In light of this, in addition to the fact that each Native API calls `KiFastSystemCall` without setting a stack frame, the application's stack during the execution of `TraceSysCallEntry` is in the following state (*Figure 3.4*).

Having outlined the general situation, it is finally possible to describe how the main image check is carried out:

1. The first check involves discovering whether or not `sysenter` is called directly from the main executable. As Pin intercepts Native APIs right before the execution of `sysenter`, this can be trivially done by checking if the instruction pointer value obtained in `TraceSysCallEntry` falls within the main executable memory address range.

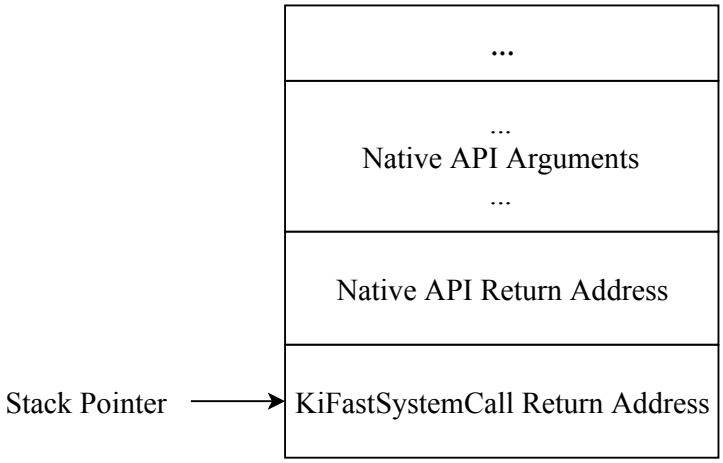

Figure 3.4. *Stack before* `sysenter` *execution*

2. Secondly, it is required to examine if the Native API return address belongs to the main executable. As a result of what shown in *Figure 3.4* such return address is obtained by adding 4 to the stack pointer and retrieving the pointed value, where the stack pointer can be obtained in Pin through the use of `PIN_GetContextReg`. The resulting value is then, once more, compared with the main executable memory address range.

3.3.2 Native API Name Resolution

Previously, it was stated how it is possible to register a callback function to be executed before Native APIs through the use of `PIN_AddSyscallEntryFunction`. Such callback functions, named `SYSCALL_ENTRY_CALLBACK`s, receive a set of parameters, including `ctx`, the application's register state immediately before the system call execution, and `std`, the system call standard. In BluePill, these two parameters are used to invoke `PIN_GetSyscallNumber` inside its `SYSCALL_ENTRY_CALLBACK`. Such API returns the number (ID) of the Native API to be executed in the provided context [27].

BluePill employs a mechanism which allows it to obtain the Native API name from its number, since the hooking functions it employs are indexed by name and not by ordinal. This choice was made because the identifiers vary depending on the Windows version, even among different Service Pack versions. For the same reason,

the information needed by BlueTracer to correctly log Native APIs is also indexed by Native API name and, consequently, BlueTracer also utilizes the aforementioned Native API name resolution mechanism.

The idea is to create an array, named `syscallIDs`, where Native API names are indexed by their IDs, by parsing `ntdll`'s export information. The export data of a PE is stored in the `IMAGE_EXPORT_DIRECTORY` structure located in the header. In our case, the most relevant fields of this structure are:

- The `AddressOfFunctions` array, which contains RVAs [1] pointing to the actual exported functions and is indexed by an export ordinal.
- The `AddressOfNames` array, which is an array of 32-bit RVAs pointing to symbol strings.
- The `AddressOfNameOrdinals` array, which is an array of 16-bit ordinals existing in parallel with `AddressOfNames`, i.e. they possess the same number of elements and there is a direct relation between equivalent indices [32].

With this in mind, `syscallIDs` is built by carrying out the following actions for every element `iName` in `AddressOfNames`:

1. The corresponding `AddressOfNameOrdinals` element is retrieved, i.e. the one with the same index. Let us call this value `iOrdinal`.
2. `iOrdinal` is used to index in `AddressOfFunctions`. This time the obtained value is the RVA pointing to the exported function.
3. The pointed function is expected to begin `mov eax, syscall_number`. As a result of this, the first byte should be `B8h` and the syscall number can be obtained by considering the next four bytes.

By following the above procedure, every element in `AddressOfNames` can be therefore mapped to the corresponding identifier.

[1] A RVA (Relative Virtual Address) is essentially an offset within the PE image in memory

3.3.3 Native API Information Representation and Retrieval

When tracing Native APIs, it is wanted to record as much data as possible as well as correctly formatting the arguments' values. To do this, it is required to have access to some kind of source of Native API related information, which can assist the tracer in the logging activity by, for example, providing the number of arguments a Native API takes as input, listing the arguments' types and differentiating between input and output arguments. In BlueTracer, this information was adapted from the Native API data provided by Dr.Memory [14], a memory monitoring tool based on the DynamoRIO DBI framework.

For each Native API, the information related to it is contained in a `struct` of type `syscall_info_t` (*Listing 3.2*). Most fields of such `struct` are self-explanatory. In particular, `num` is a `struct` storing two values indicating the system call number; these are filled in dynamically by Dr.Memory but are not needed by BlueTracer. Furthermore, the `flags` field is utilized to notify whether or not all the details of the Native API are known, as most Native APIs are undocumented. Undoubtedly though, a major role is played by the `arg` array, which is made up by `sysinfo_arg_t` `structs` (*Listing 3.2*) containing the data of the Native API arguments. This array is initialized with size `MAX_ARGS_IN_ENTRY` (i.e. 18), since a Native API can have at most 18 arguments.

```
1   typedef struct _syscall_info_t {
2
3       drsys_sysnum_t num;         // Native API ID
4       const char *name;           // Native API Name
5       uint flags;                 // SYSINFO_ flags
6       uint return_type;           // Return type
7       int arg_count;              // Number of arguments
8
9       // Array of arguments
10      sysinfo_arg_t arg[MAX_ARGS_IN_ENTRY];
11      ...
12  } syscall_info_t;
```

Listing 3.2. `struct` containing Native API-related information

```
1  typedef struct _sysinfo_arg_t {
2      int param;                  // Parameter Ordinal
3      int size;                   // Size
4      uint flags;                 // SYSARG_ flags
5      int type;                   // Type
6      const char *type_name;      // Symbolic Name of the arg Type
7  } sysinfo_arg_t;
```

Listing 3.3. `struct` containing information associated to a Native API argument

In `sysinfo_arg_t`, other than `param` and `size`, that are straightforward, the following fields are also present:

- `flags`, which stores an `OR` of flags describing the argument's characteristics. The most important ones are:
  - `SYSARG_READ (R)` : input argument.
  - `SYSARG_WRITE (W)` : output argument.
  - `SYSARG_INLINED` : non-memory argument, i.e the whole value is in parameter slot.
  - `SYSARG_HAS_TYPE (HT)` : argument with a type specifier. In fact, a non `SYSARG_INLINED` argument is by default of type `struct` (`DRSYS_TYPE_STRUCT`), unless specified otherwise by `SYSARG_HAS_TYPE`.
- `type`, which is an `enum` value indicating the data type of the parameter
- `type_name`, a string indicating the symbolic name of the `arg` type, which is typically filled dynamically based on the `type` value. In case the argument value is a named constant, the `type_name` field contains the name of the enumeration the constant belongs to. In fact, for each one of these enumerations, BlueTracer has access to a `struct` specific for that enumeration containing the constant values and their corresponding name. This information was also provided by Dr.Memory and is employed to translate constants to the appropriate name, as it will be explained in the next section.

To make things clearer, an instance of `syscall_info_t` for the Native API `NtAllocateVirtualMemory` was provided in the listing below (*Listing 3.4*).

```
1    { { 0,0 },"NtAllocateVirtualMemory", OK, RNTST, 6,
2    {
3        { 0, WIN_SIZE(HANDLE), SYSARG_INLINED, DRSYS_TYPE_HANDLE },
4        { 1, WIN_SIZE(PVOID), R | WR | HT, DRSYS_TYPE_POINTER },
5        { 2, WIN_SIZE(ULONG), SYSARG_INLINED, DRSYS_TYPE_UNSIGNED_INT },
6        { 3, WIN_SIZE(ULONG), R | WR | HT, DRSYS_TYPE_UNSIGNED_INT },
7        { 4, WIN_SIZE(ULONG), SYSARG_INLINED, DRSYS_TYPE_UNSIGNED_INT, "MEM_COMMIT" },
8        { 5, WIN_SIZE(ULONG), SYSARG_INLINED, DRSYS_TYPE_UNSIGNED_INT, "PAGE_NOACCESS" },
9    }
```

Listing 3.4. Instance of `syscall_info_t` relative to `NtAllocateVirtualMemory`

In *3.2.2* it was explained how BlueTracer obtains a Native API name from its ID. After that, as shown in *Figure 3.3*, there must be a way to, given a specific Native API name, retrieve the corresponding `syscall_info_t struct`. This is done by building an hash map during the tool's initialization which maps the Native API name to the appropriate `struct`. Such idea is also adopted for named constants enumerations since a hash map is also constructed with the objective of associating the name of a named constant enumeration to the corresponding `struct`.

3.3.4 Native API Logging

With reference to *Figure 3.3*, let us consider the point in `TraceSysCallEntry` where the `syscall_info_t struct` relative to the Native API being traced was successfully retrieved. Before describing how the logging of "known" Native APIs is performed, it is worth mentioning that, in case a `struct` describing a certain Native API is not found, BlueTracer just logs the name of the Native API and the input value of a user-specified number of arguments (4 by default).

The first step towards logging "known" Native APIs is allocating and initializing a `syscall_tracer struct` (*Listing 3.5*) representing the specific Native API being traced. This `struct` is built starting from the data present in the previously retrieved `syscall_info_t struct` and it is at the heart of the logging of the Native API.

```
1   typedef struct _syscall_tracer {
2       ADDRINT syscall_number;         // Native API ID
3       const char * syscall_name;      // Native API Name
4       int argcount;                   // Number of Arguments
5
6       // Array of arguments
7       drsys_arg_t arguments[MAX_ARGS_IN_ENTRY];
8
9       drsys_arg_t retval;             // Return value
10      int syscall_counter;            // Native API Counter
11  } syscall_tracer;
```

Listing 3.5. `struct` representing the Native API being traced

Even for `syscall_tracer`, each field is self-explanatory. The only one which was not encountered before is the `syscall_counter` field. The rationale behind this field is that, in the log, each traced call has a unique integer associated to it, utilized to group together the information relative to the call in post-processing. The next identifier to be assigned is stored in the `call_number` field of the thread local storage (*Listing 3.1*). Therefore, `syscall_counter` simply contains the unique identifier associated to the Native API in the log. The arguments of a specific Native API are represented via the `drsys_arg_t` struct (*Listing 3.6*). `drsys_arg_t`'s fields are mostly the same of `sysinfo_arg_t`, with three additions:

- `pre`, which is a boolean flag set to `true` when the logging is occurring before the Native API is executed (i.e. in `TraceSysCallEntry` and set to false when the logging is occurring after the Native API is executed (i.e. in `TraceSysCallExit`).
- `enum_name`, a string containing the symbolic name of the enumeration a named constant belongs to. In most cases, this is the symbolic name associated to the first constant of the enumeration. Such field was introduced to decouple type name and enumeration name.
- `value`, an `ADDRINT`[2] containing the value of the argument. This is obtained

[2]The ADDRINT type is defined by Pin and represents a memory address

through the `PIN_GetSyscallArgument` API, which takes as input the context before the execution of the system call, the system call standard and the ordinal number of the argument whose value is requested.

```
typedef struct _drsys_arg_t {

    // Whether operating pre-call (if true) or post-system call (if false)
    bool pre;

    int ordinal;                // Parameter Ordinal
    int size;                   // Size
    uint flags;                 // SYSARG_ flags
    int type;                   // Type
    const char *type_name;      // Symbolic Name of the arg Type

    // String describing the symbolic name of a named constant's enum
    const char *enum_name;

    // Argument value
    ADDRINT value;

} drsys_arg_t
```

Listing 3.6. `struct` representing an argument of the Native API being traced

As previously mentioned in section 3.1.1, each thread possesses its own log file, whose pointer resides in the thread local storage, and writes on it by means of the `file_write` function, also located in the thread local storage (*Listing 3.1*). The first Native API component being logged is its name and this is done with the following format:

`~~[System ID of thread]~~ [Call Counter] [Image Name]![Native API Name]`

In the context of Native APIs, the name of the image is always `ntdll`, but this is not the case when tracing APIs.

Argument logging is done via the `print_arg` function (*Listing 3.7*), which is structured as follows:

- Firstly, it is determined if the argument being logged is a named constant,

i.e. it is checked if `enum_name` is different from `NULL`. In that case, the `get_arg_syname` function is invoked, which is in charge of, given the input named constant value, finding the corresponding name and recording it to the log. The named constant resolution is carried out by initially fetching the `struct` containing all the members of the enumeration the named constant belongs to, through the use of the aforementioned hash map. Then, it is determined if there is a perfect match between the argument value and one of the values of the `struct`'s entries. If this occurs, then the associated symbolic name is simply retrieved from the `struct`'s entry. Otherwise, a linear search is performed to unveil possible composite named constants (e.g. `FILE_SHARED_READ | FILE_SHARED_WRITE`).

- Then, if the argument's type is primitive (e.g. `int`, `bool`, etc.), `print_simple_value` is invoked to record its value. In particular the second parameter of this function is a boolean which is set to `true` if it is wanted to print the argument's value with leading zeros (e.g. if the argument is of pointer type and the address it stores is being logged) and `false` otherwise. The way `print_simple_value` operates is quite straightforward:

  1. At the beginning the argument's value is simply logged, with leading zeroes or not depending on the previously mentioned parameter
  2. Then, if the argument is a pointer, it is determined if the value it points to needs to be logged. This occurs if the argument is being processed before the Native API execution (i.e. `pre` is `true`) and is an input parameter (i.e. SYSARG_READ is contained in `flags`) or if the argument is being processed after the Native API execution (i.e. `pre` is `false`) and is an output parameter (i.e. SYSARG_WRITE is contained in `flags`). The pointed value is obtained through the use of `PIN_SafeCopy`, which copies the specified number of bytes from a source memory region to a destination memory region, guaranteeing safe return to the caller even if such regions are inaccessible.

```
1  static void print_arg(drsys_arg_t* curr_arg, bluepill_tls* tdata, uint syscall_counter) {
2
3      ...
4
5      // Constant Resolution
6      if (curr_arg->enum_name != NULL) {
7          if (get_arg_symname(curr_arg, tdata))
8              return;
9      }
10
11     switch (curr_arg->type) {
12         case DRSYS_TYPE_VOID:         print_simple_value(curr_arg, true, tdata); break;
13         case DRSYS_TYPE_POINTER:      print_simple_value(curr_arg, true, tdata); break;
14         case DRSYS_TYPE_BOOL:         print_simple_value(curr_arg, false, tdata); break;
15         case DRSYS_TYPE_INT:          print_simple_value(curr_arg, false, tdata); break;
16         case DRSYS_TYPE_SIGNED_INT:   print_simple_value(curr_arg, false, tdata); break;
17         case DRSYS_TYPE_UNSIGNED_INT: print_simple_value(curr_arg, false, tdata); break;
18         case DRSYS_TYPE_HANDLE:       print_simple_value(curr_arg, false, tdata); break;
19         case DRSYS_TYPE_NTSTATUS:     print_simple_value(curr_arg, false, tdata); break;
20         case DRSYS_TYPE_ATOM:         print_simple_value(curr_arg, false, tdata); break;
21     default: {
22         if (curr_arg->value == 0) {
23             (tdata->file_write)(tdata->threadid, tdata->buffer, tdata->OutFile, "<null>");
24         }
25         else if (curr_arg->pre && !TEST(SYSARG_READ, curr_arg->flags)) {
26             (tdata->file_write)(tdata->threadid, tdata->buffer,
27             tdata->OutFile, PFX, curr_arg->value);
28         }
29         else {
30             if (!print_known_compound_type(curr_arg, tdata))
31                 (tdata->file_write)(tdata->threadid, tdata->buffer, tdata->OutFile, "<NYI>");
32         }
33     }
34     ...
35 }
```

Listing 3.7. `print_arg` function

- Finally, if the argument's type is not a primitive one, it is checked if it is `null` and if it is a complex output parameter being traced before the Native API execution, situation in which only the address stored in the pointer is logged. If none of these two scenarios are true, then the tracer finds itself in the situation where it is required to log the value of a complex type. This is performed through the invocation of `print_known_compound`. As of right now, such function differentiates between four complex types, namely `UNICODE_STRING`, `OBJECT_ATTRIBUTES`, `IO_STATUS_BLOCK` and `LARGE_INTEGER`, and logs the argument's value accordingly. If the argument's type is a complex type that is not supported, the symbolic value `<NYI>` (not yet implemented) is recorded.

Once the arguments' input values are logged, then the reference to the `syscall_tracer struct` representing the Native API under analysis is stored in thread local data (*Listing 3.1*). This is done so that, after the Native API's execution, the corresponding `syscall_tracer` data structure can be accessed from `TraceSysCallExit`. In fact, as mentioned in section 3.2, the `bluepill_tls struct` associated to the running thread can be retrieved in any analysis function by means of `PIN_GetThreadData`.

In `TraceSysCallExit`, after the value of `syscallEntry` has been fetched from the thread local storage, then it is determined whether the Native API has succeeded by checking if the output of `PIN_GetSyscallErrno` is equal to zero, where `PIN_GetSyscallErrno` is a Pin API returning the error code of the system call which has just returned with the provided context. Afterwards, `PIN_GetSyscallReturn` is utilized to get the return value of the Native API and, with this information, the corresponding `drsys_arg_t` data structure is built. Successively, the Native API return value is logged, together with the output arguments, using once again `print_arg` (*Listing 3.7*). Finally, the `syscall_tracer struct` representing the Native API being traced is deallocated.

To conclude this section, let us show how a traced Native API looks like in the log file (*Listing 3.8*). As it can be observed, the adopted log format is quite intuitive. In fact, the idea was to have a log which is both easy to read by the analyst but also easy to parse and post-process.

```
~~2868~~ 1072 ntdll.dll!NtOpenFile
1072    arg 0: 0x000fe810 (type=HANDLE*, size=0x4)
1072    arg 1: 0x100020 (type=unsigned int, size=0x4)
1072    arg 2: len=0x18, root=0x0, name=210/538 "\??\C:\Windows\WinSxS\
        x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.23894_none_5c0be957a009922e",
        att=0x40, sd=0x00000000, sqos=0x00000000 (type=OBJECT_ATTRIBUTES*, size=0x4)
1072    arg 3: 0x000fe7c0 (type=IO_STATUS_BLOCK*, size=0x4)
1072    arg 4: FILE_SHARE_READ|FILE_SHARE_WRITE (type=named constant, value=0x3, size=0x4)
1072    arg 5: FILE_DIRECTORY_FILE|FILE_SYNCHRONOUS_IO_NONALERT
        (type=named constant, value=0x21, size=0x4)
1072    succeeded =>
1072    arg 0: 0x000fe810 => 0x58 (type=HANDLE*, size=0x4)
1072    arg 3: status=0x0, info=0x1 (type=IO_STATUS_BLOCK*, size=0x4)
```

Listing 3.8. Log entry relative to a `NtOpenFile` call

3.4 APIs Tracing

In Microsoft Windows, APIs are implemented as functions provided by a set of dynamic-link libraries. These, also known as DLLs, constitute Microsoft's way of implementing the concept of shared libraries in the Windows operating system. Therefore, the functions they make available can be employed by different applications [17]. Windows APIs offer a plethora of functionalities which belong to many different categories, ranging from base services (e.g. file management) to user interface functions and network operations [10]. In light of this, a Windows API has rich semantic information associated to it and tracing the sequence of APIs a malware calls provides analysts with a very high-level view of the sample's behavior. This is why BlueTracer's API tracer component is undoubtedly the most important one. When tracing APIs, most of the concepts seen in Native API tracing also apply, but there are also significant differences, both in the steps that were carried out and in the Pin APIs which were employed, as it can be observed from the diagram in *Figure 3.5*.

Now let us illustrate the actions being performed during API tracing by analyzing in detail each one of the three main blocks of *Figure 3.5*.

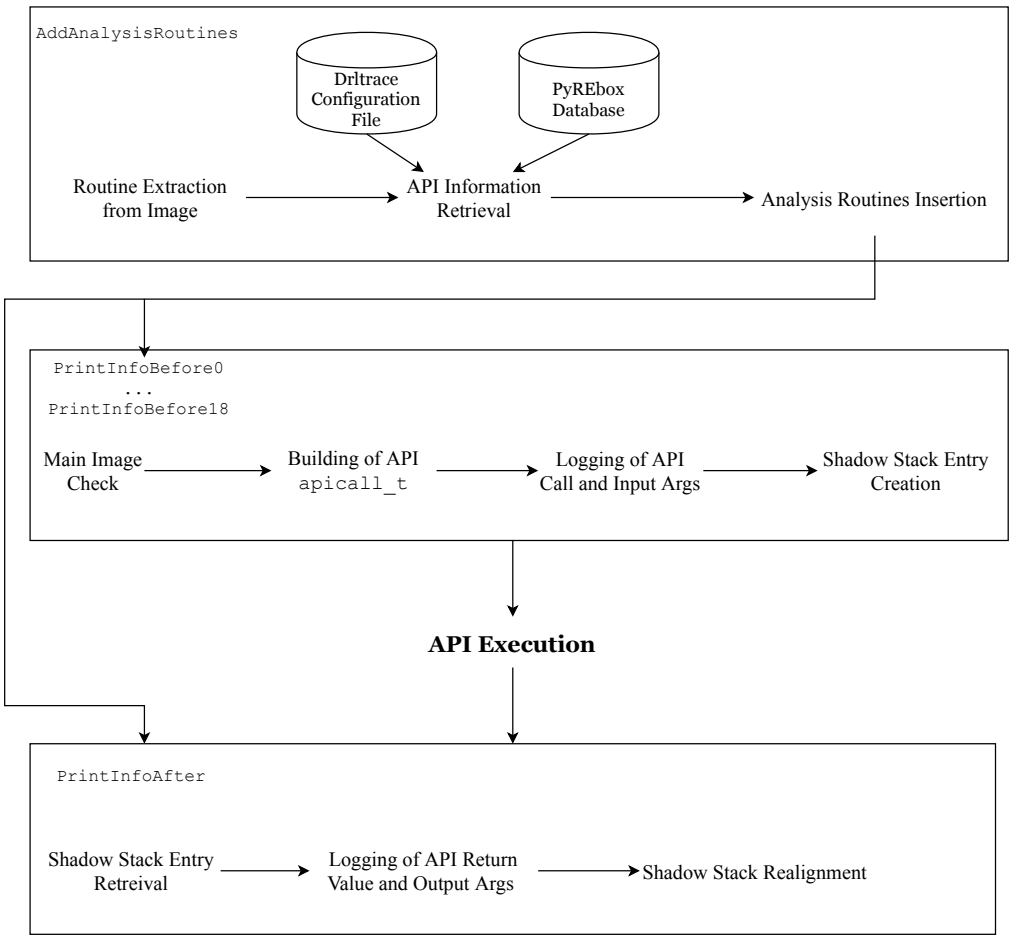

Figure 3.5. *APIs Tracing Workflow*

3.4.1 APIs Instrumentation

The first step taken towards APIs tracing is APIs instrumentation, i.e. placing analysis routines before and after the APIs' execution. To do this, a specific function was embedded in BluePill's image callback (the notion of image callback was previously introduced in Section 3.3.1). Such function, named `AddAnalysisRoutines`, performs the following actions for every DLL being loaded:

1. It inspects the symbol table, i.e. the DLL's exports. To this end, Pin symbol objects (`SYM`s) are employed, which provide information about function symbols in the applications [27].

2. For every symbol object, it retrieves the corresponding routine (`RTN`) object. In

fact, in Pin a `RTN` represents a function usually generated by a compiler for a procedural programming language, e.g C [27]. To retrieve the aforementioned `RTN` object, the `RTN_FindByAddress` API was utilized, which takes as input a `RTN` memory address and returns an handle to the found `RTN`. Such memory address was determined by adding the symbol's RVA (obtained via `SYM_Value`) to the lowest image address (fetched through `IMG_LowAddress`).

3. For every routine object, it retrieves the corresponding name via `RTN_name` and checks whether or not the API being represented is "known", i.e. a source of information associated to the API exists.

   - If the API is not "known", it adds an analysis routine just before the API's execution, which simply logs the value of a user-specified number of args (four by default), exactly like what happens in NTAPIs tracing.
   - If the API is "known", it adds analysis routines before and after the API's execution, which log detailed information relative to the API, including the arguments' input and output values.

Having given a general outline on how `AddAnalysisRoutine` works, let us now describe its underlying details.

Similarly to what occurs for NTAPI tracing, in order to log as much information as possible and to correctly record the arguments' values, it is necessary to have a source of API information, providing some kind of assistance during the tracing activity. When dealing with APIs, BlueTracer allows the user to choose between two possible sources of API information: *drltrace*'s configuration file or the data extracted from *PyREbox*'s database. By default, the latter is employed as it embodies a greater amount of information, including variable names and named constants' enumerations.

drltrace (already mentioned in section 2.3) comes with its own external configuration file, in which each line contains information relative to an API, as it can be observed from the sample configuration file entry below (*Listing 3.9*).

```
bool|GetUILanguageInfo|DWORD|wchar*|__out wchar*|__inout DWORD*|__out DWORD*
```

Listing 3.9. Sample entry in *drltrace* configuration file

Each piece of information in an entry is separated by `|`. The first bit of data is the API's return type, the second is the API's name and the rest of the entry is made up by the arguments' types. In particular, the `__out` token is used to mark output arguments, while `__inout` is utilized to identify input and output arguments. In case there is no token, it means that the argument is just an input one.

Before API instrumentation takes place, BlueTracer parses the aforementioned configuration file and, for every entry, builds a `sysinfo_arg_t struct` (*Listing 3.2*) for each argument in the entry. It was decided to reuse `sysinfo_arg_t struct` since its fields were fitting with respect to the arguments' information which had to be stored. Therefore, after this parsing process, each configuration file entry is represented by an <API name, `vector` of `sysinfo_arg_t`s> pair. Such pairs are then utilized to build an hash map, which maps the API name to the corresponding arguments. This hash map is used in step 3 of the APIs instrumentation process to, given the API name, fetch the appropriate information. In particular, it is important to note that, from a performance point of view, it is much better to include the information retrieval operations in the image instrumentation function, rather than in the analysis ones, as the former are executed just once for every image, while the latter are invoked each time an API is called by the pinned application.

The other source of API information employed by BlueTracer is *PyREbox*'s database. *PyREbox* is a Python scriptable reverse engineering sandbox based on QEMU and VMI techniques, the goal of which is to provide support for reverse engineering through its dynamic analysis capabilities [30]. *PyREbox* is equipped with its own API tracer, which relies on the information contained in a sqlite database to correctly log the APIs' parameters. Such database was, in turn, generated by utilizing as its core the data from the *Deviare*[3] project and then employing a crawler for parsing the Microsoft online documentation with the goal of marking which parameters are input parameters and which are output parameters. The resulting

[3]Deviare is an open-source hooking engine for instrumenting arbitrary `Win32` functions [13]

database is incredibly richer in API information than *drltrace*'s configuration file. In fact, the number of APIs for which data is stored is much higher, argument names are also included, as well as the contents of named constants' enumerations, information which *drltrace*'s configuration file does not provide at all.

In order to extract information relative to the APIs from PyREbox's database, a Python script was employed, which, for every API, instantiates a `libcall_info_t struct` (*Listing 3.10*) in a `.cpp` file.

```
1 typedef struct _libcall_info_t {
2     const char* func_name;              // API name
3     int argnum;                         // Number of Args
4     libcall_arg_info_t lib_args[19];    // Array of arguments
5 } libcall_info_t
```

Listing 3.10. `struct` containing API-related information from PyREbox's database

The most important field of such `struct` is surely the arguments' array, which is made up of `libcall_arg_info_t` data structures (*Listing 3.11*) containing the information relative each argument of an API, including an entry specific for the return value data. The array size was set to 19, since it was observed from the database data that the API with the most parameters had 18 arguments. This time, it was decided not to reuse NTAPI's `sysinfo_arg_t struct` (*Listing 3.2*) to store the API's arguments information due to its lack of the field storing the argument name.

```
1 typedef struct _libcall_arg_info_t {
2     int arg_num;                // Arg Ordinal
3     const char* arg_name;       // Arg Name
4     int arg_type;               // Arg Type
5     char* arg_type_name;        // Arg Type Name
6     int size;                   // Size
7     bool in_out_flag;           // Input/Output Flag
8 } libcall_arg_info_t;
```

Listing 3.11. `struct` containing information associated to an API argument

Although `libcall_arg_info_t`'s fields seem to be pretty self-explanatory, let us quickly go through them to reveal some details which are not so obvious:

- `arg_num` is an `int` which contains the argument's ordinal. In case the return value is being represented, it is set to -1.
- `arg_name` is a string containing the argument name as reported by Microsoft's official documentation.
- `arg_type` is an `int` from an enumeration representing the argument's type. In particular, differently from the strategy adopted from Native APIs, in case of a pointer the `NKT_DBOBJCLASS_Pointer` enumeration member is ORed with an `int` representing the pointed type. The same thing happens in case of a pointer to a pointer but with the `NKT_DBOBJCLASS_PointerPointer` flag being used instead. This was done to reflect how API information is stored inside the database.
- `arg_type_name` is a string which is used in the three specific scenarios below, according the type of the argument, and is `null` otherwise:
  1. To store the symbolic name of an enumeration.
  2. To store the `struct` type name.
  3. To store the `union` type name.
- `size` is an `int` storing the argument's size. In case of a pointer (or a pointer to a pointer) the size of the pointed type is stored.
- `in_out_flag` is a `bool` which is set to `INOUT` (i.e `true`) if the represented argument is an output argument and `IN` (i.e. `false`) otherwise. This means that, by default, all the arguments are considered as input arguments and are therefore traced before the API execution, while only the arguments for which `in_out_flag` is `true` are traced after the API's execution.

To give a better idea on how API data is represented, an instance of `libcall_arg_info_t` containing the information associated to `WriteFileEx` can be observed below (*Listing 3.12*).

```
1   { "WriteFileEx",5,
2   {
3       {-1, "Return value", NKT_DBFUNDTYPE_SignedDoubleWord, 0, 4, INOUT },
4       {0, "hFile", NKT_DBFUNDTYPE_UnsignedDoubleWord, 0, 4, IN },
5       {1, "lpBuffer", NKT_DBFUNDTYPE_Void | NKT_DBOBJCLASS_Pointer, 0, 0, IN },
6       {2, "nNumberOfBytesToWrite", NKT_DBFUNDTYPE_UnsignedDoubleWord, 0, 4, IN },
7       {3, "lpOverlapped", NKT_DBOBJCLASS_Struct | NKT_DBOBJCLASS_Pointer,
8        "_OVERLAPPED", 160, INOUT },
9       {4, "lpCompletionRoutine", NKT_DBOBJCLASS_Typedef, 0, 0, IN },
10  }
11  }
```

Listing 3.12. Instance of `libcall_arg_info_t` relative to `WriteFileEx`

Due to the high amount of APIs for which information was stored in the `PyREbox` database, it was decided to group API data by DLL. Specifically, for every DLL a corresponding `.cpp` file was created to store the API-related information under the form of `libcall_arg_info_t` instances, one for each "known" API exported by that DLL. Furthermore, in order to make API data retrieval more efficient, it was chosen to employ a two-level hash map approach for this purpose. Given the DLL name (easily obtainable in the image callback via the use of `IMG_Name`), the first level hash map is utilized to retrieve the DLL-specific second level hash map, which, in turn, maps the API name to the appropriate `struct` instance (*Figure 3.6*). This is how API information retrieval is carried out in case *PyREbox* database is used as API data source.

Let us conclude this section by explaining how analysis routines are inserted before and after the API execution during the API instrumentation procedure outlined in pages 34-35. In BlueTracer such operation heavily relies on the use of the `RTN_InsertCall`, which allows to insert analysis functions relative to a `RTN` object.

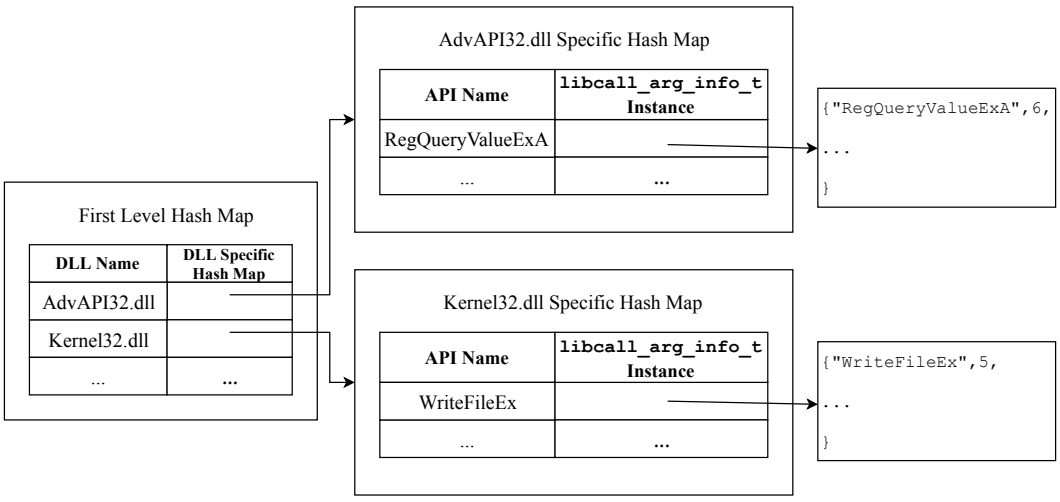

Figure 3.6. *PyREbox API Information Retrieval*

This API takes as input the following parameters:

- The routine object (`RTN`) representing the function under analysis.
- A member of the `IPOINT` enumeration which determines where the analysis function is inserted in relation to the instrumented object. It can be either `IPOINT_BEFORE`, in which case the analysis code is placed before the instrumented function, or `IPOINT_AFTER`, in which case the analysis code is placed after the instrumented function.
- The analysis function to be called.
- The arguments to pass to the analysis function, specified via members of the `IARG_TYPE` enumeration. If the analysis function is placed before the instrumented object, then such arguments may also include the parameters' values of the function being instrumented. However, for this to occur the pair <`IARG_FUNCARG_ENTRYPOINT_VALUE`, argument number> needs to be included for each of the analyzed function's parameters. Conversely, to obtain the instrumented function's result, `IARG_FUNCRET_EXITPOINT_VALUE` is required. Obviously, this is possible only if the analysis function is placed after the instrumented object.

In BlueTracer, the number of arguments of the API being traced is known only after the API-related information has been retrieved. Because of this and given Pin's way of passing the arguments to the analysis functions, a `switch` had to be employed when adding analysis functions before the API execution. Such `switch`, given the API arguments' number, places the appropriate analysis function, i.e. the one with the number of <`IARG_FUNCARG_ENTRYPOINT_VALUE`, argument number> pairs equal to the number of arguments the API takes. This is done in order to ensure that the analysis function receives all the values of the API's arguments before the API's execution. As a result, in BlueTracer there are 19 (one for zero arguments as well) different API `IPOINT_BEFORE` analysis functions, named `PrintInfoBefore[Arguments' Number]`, which vary only in the number of APIs' argument values they receive in input. Obviously this is true just for "known" APIs. In case the API under analysis is not "known", then the number of API argument values is always the same and the `switch` is not required.

Let us now dissect an invocation of `RTN_InsertCall` to further clarify how BlueTracer adds analysis code before the execution of an API (*Listing 3.13*).

```
1 RTN_InsertCall(rtn, IPOINT_BEFORE, (AFUNPTR)PrintInfoBefore[Number of API Args],
2     IARG_FAST_ANALYSIS_CALL,
3     IARG_ADDRINT, argNumber,
4     IARG_ADDRINT, libPointer, IARG_ADDRINT, rtn_name, IARG_ADDRINT, img_name,
5     IARG_REG_VALUE, REG_STACK_PTR,
6     IARG_THREAD_ID,
7     IARG_RETURN_IP,
8     [Number of API Args]_ARGS
9     IARG_END);
```

Listing 3.13. `RTN_InsertCall` invocation to add analysis code before an API's execution

In particular, the arguments which are passed to the analysis routine are:

- `IARG_FAST_ANALYSIS_CALL`. This is not a real argument but rather a way to enable faster linkage for calls to analysis functions with the objective of improving performance [27].

- `argNumber`, a constant value containing the number of the analyzed API's arguments.
- `libPointer`, a reference to the previously retrieved data structure containing API-related data.
- `rtn_name`, the API name.
- `img_name`, the DLL name.
- The stack pointer value before the API's execution, given by the `<IARG_REG_VALUE, REG_STACK_PTR>` pair. This is necessary for the shadow stack management, which will be detailed in the next section.
- The thread ID assigned by Pin for the calling thread, passed via `IARG_THREAD_ID`. This is necessary in order to access the thread local storage from the analysis function.
- The API return address, provided by `IARG_RETURN_IP`. This is employed in the main image check, similarly to what explained in Section 3.3.1.
- The API argument values. In order to make the code more readable a macro was used in this case.

For what concerns the addition of analysis code after the API's execution, the aforementioned `switch` is not necessary since `IARG_FUNCRET_EXITPOINT_VALUE` is valid only at the entry point of an analysis routine and, therefore, no API argument value is passed at this stage. The analysis function which is placed after the API's execution, named `PrintInfoAfter` essentially receives the same parameters as the ones from *Listing 3.13*, with the major difference that the API's return value is passed via `IARG_FUNCARG_EXITPOINT_VALUE` instead of the API arguments' values.

3.4.2 API Analysis before Execution

In this section we will describe how APIs are analyzed before execution, i.e. the main steps that are carried out in the `PrintInfoBefore` functions, an overview of which is given in *Figure 3.5*. The workflow in this case is mostly the same as the

one for NTAPIs' analysis, with one major difference, that is the introduction of a shadow stack used to store API entries in the thread local storage, which will be motivated later in the section.

The first thing which is done is determining whether or not the API under analysis has been invoked directly from the main executable of the Pin application. The concepts involved here are essentially the ones applying to the main image check done for Native APIs, which was detailed in *Section 3.3.1*. In short, it is checked if the API's return address, which is passed to the analysis function through the use of `IARG_RETURN_IP`, falls into the main executable memory address range, which was previously determined via `IMG_HighAddress` and `IMG_LowAddress`.

Afterwards, similarly to what occurs when logging "known" Native APIs, a `apicall_t struct` (*Listing 3.14*) representing the specific API being traced is allocated and initialized. The fields of such `struct` are all trivial and, as what done for Native API tracing, the API arguments are represented via a `drsys_arg_t` (*Listing 3.6*) array with size `MAX_ARGS_CONFIG` (i.e. 18) as this is the maximum number of observed arguments for any "known" API. In particular, the `drsys_arg_t struct` could be reused in the context of APIs since, unlike `sysinfo_arg_t`, its fields could hold all API arguments' data, both from the *drltrace* configuration file and the *PyREBox* database, including the argument name.

```
1  typedef struct _apicall_t {;
2
3      const char* img_name;                          // DLL Name
4      const char* rtn_name;                          // API Name
5
6      drsys_arg_t arguments[MAX_ARGS_CONFIG];        // Array of Arguments
7      drsys_arg_t retval;                            // Return Value
8      int count;                                     // Arg Count
9
10 } apicall_t;
```

Listing 3.14. `struct` representing the API being traced

The `apicall_t struct` is initialized utilizing the API-related data, which was fetched beforehand during instrumentation and was passed to the analysis function via `libPointer`, as well as the values of the API arguments, which were provided to the analysis function through `IARG_FUNCARG_ENTRYPOINT_VALUE` as already discussed in *Section 3.4.1*.

Then, the logging of the API proceeds exactly the same as for Native APIs: the API call is recorded employing an identical log format in order to maintain uniformity and the input values of the arguments are logged through the use of a `print_arg` function operating exactly in the same way as the one in *Listing 3.7*.

As previously hinted at, the major element which distinguishes API tracing from Native API tracing is that the former employs a shadow stack to store in the thread local storage references to the data structures representing the APIs being traced. Let us explain in detail the motivation behind such choice. It is typical for an API to call another API during its execution, forming a sort of nesting. For this reason, just storing in the thread locale storage the reference relative to the next API to be executed is not enough as this would lead to the analysis of just the most "inner" API, completely ignoring the "outer" APIs which invoked the "inner" one. Therefore, it is necessary to store not just the reference corresponding to the next API in line to be executed but rather all the references relative to the APIs for which execution has started and not yet finished. A fitting data structure to solve this issue is a shadow stack, where, for each API, the corresponding data structure is placed on top of the stack before its execution and popped from the stack after its execution has terminated, allowing both "inner" and "outer" APIs to be traced. This is why each thread has access to its own shadow stack via the `shadowStack` field in the thread local data (*Listing 3.1*).

Therefore, in light of what just stated, the last operations which are done when tracing an API before its execution are allocating a shadow stack entry (*Listing 3.15*), initializing it and placing it on top of the shadow stack in the thread local data, so that it can be retrieved after the API's execution.

```
1 typedef struct _stackEntry {
2     apicall_t* apiInfo;    // API Call Reference
3     ADDRINT  currentSP;    // Stack Pointer Register Content
4     THREADID threadID;     // Thread ID
5     uint api_counter;      // Call Counter
6 } stackEntry;
```

Listing 3.15. `struct` representing a shadow stack entry

`stackEntry`'s fields are all, once again, self-explanatory. A big role in the shadow stack management is taken by the `currentSP` field, as it will be explained in the next section. Such field stores the stack pointer's value before the API's execution, which was passed to the analysis function with the <`IARG_REG_VALUE`, `REG_STACK_PTR`> pair.

3.4.3 API Analysis after Execution

Lastly, let us detail the most important operations performed towards tracing API-related information after the API execution. These are carried out in the `PrintInfoAfter` function and can be observed from *Figure 3.5*.

At the beginning of `PrintInfoAfter`, the first thing which needs to be done in order to proceed with the logging is the retrieval from the shadow stack of the stack entry representing the API under analysis. A reference to the shadow stack can be easily acquired by gaining access to the thread local storage via `PIN_GetThreadData`. However, it is not enough to pop the top of the shadow stack to obtain the wanted stack entry. This is due to a limitation of Pin in the instrumentation of routine objects.

In fact, the addition of analysis routines after a function's execution with `IPOINT_AFTER` is implemented by instrumenting each return instruction. This does not guarantee the success of the instrumentation, meaning that, for some routines, the associated `IPOINT_AFTER` analysis function is not executed. Therefore, in our case, it is possible that the stack entry on top of the shadow stack refers to API for which `PrintInfoAfter` has not been invoked and, therefore, the corresponding stack entry has not been popped.

As a result of this, the correct stack entry has to be fetched by iterating through the shadow stack, looking for the entry for which the values of a set of fields coincide with the values of the corresponding parameters being passed as arguments to the analysis function. Such fields are:

- The DLL name.
- The API name.
- The stack pointer value. In fact, for a given API, the stack pointer value before its execution has to be equal to the stack pointer value after its execution.

Once the appropriate shadow stack entry has been retrieved, the API return value, which is passed to the analysis function via `IARG_FUNCARG_EXITPOINT_VALUE`, is set in the `apicall_t struct` so that it can be logged, together with the output arguments, once again utilizing the ideas behind `print_arg` (*Listing 3.7*).

The last operation carried out by `PrintInfoAfter`, after the API under analysis has been traced, is the re-alignment of the shadow stack, i.e. the deallocation of all the stack entries belonging to APIs which have terminated their execution. In fact, due to the previously mentioned issue involving Pin's instrumentation of routines, it is necessary to manually remove from the shadow stack all the entries relative to the APIs for which the corresponding `IPOINT_AFTER` analysis function is not executed. Such shadow stack re-alignment procedure works as follows:

1. The previously fetched shadow stack entry is removed.
2. All the shadow stack entries on top of the previously retrieved entry are removed. Due to their position in the stack, these entries are relative to APIs which have been called after the traced API. Such APIs, given the fact that the traced API has terminated its execution, have also finished to execute, but their relative entries have not been deallocated accordingly due to Pin's issue with routine instrumentation.
3. All the entries with a lower stack pointer value than the stack pointer value stored in the retrieved entry are removed. In fact, such entries refer, once

again, to APIs which have been invoked before the traced APIs but their corresponding entries have not been deallocated accordingly.

3.5 Context Change Analysis

Pin has to intercept the delivery of asynchronous events from the kernel in order to keep control of the application. Microsoft Windows employs two mechanisms aimed at dispatching asynchronous events to user mode, i.e. callbacks and asynchronous procedure calls (APCs), both of which lead to a context change in the application [33].

In order to have a complete picture of the malware sample's activity, it is clearly relevant to also log the occurrences of such asynchronous events and to record as much information as possible related to them. Luckily, Pin provides an API which perfectly meets these needs, named `PIN_AddContextChangeFunction`.

This API allows to register a notification function to execute just before the pinned application changes context due to the reception of an asynchronous event, like for instance a callback or a Windows APC. In BlueTracer, the idea is to use such registered notification function to extract and log information relative to the context change. The notification function in question is of type `CONTEXT_CHANGE_CALLBACK` and the most important arguments it takes as input are:

- A member of the `CONTEXT_CHANGE_REASON` enumeration indicating the reason for the context change. This is the parameter allowing BlueTracer to distinguish between callbacks and APCs. In fact, in the case of callbacks it is set to `CONTEXT_CHANGE_REASON_CALLBACK`, while in the case of APCs it is set to `CONTEXT_CHANGE_REASON_APC`.

- The application's register state before the context change. It is `null` if the context change is caused by a callback.

- The application's register state after the context change.

Having outlined the tools made available by Pin to deal with the application's context changes, let us now explain in detail how callbacks tracing and Windows

APCs tracing is carried out in BlueTracer.

3.5.1 Callbacks Tracing

The Windows kernel frequently needs to make callbacks in user mode with the goal of carrying out specific tasks, such as the invocation of hooks defined by the application, the provision of event notifications and the exchange of data with user mode. These calls are commonly referred to as user mode callbacks [23].

To make calls from user mode to kernel mode, the user mode callback dispatcher (`KiUserCallbackDispatcher`) is employed. This function takes two arguments, a number indicating the callback to be invoked and a structure pointer which the callback receives as input, containing several parameters packed in a contiguous memory block [2]. `KiUserCallbackDispatcher` operates in the following way:

1. It accesses the `KernelCallbackTable` in the process environment block (PEB) [4]. The `KernelCallbackTable` is an array of function pointers, where each entry contains a reference to a callback routine [9].

2. It uses the callback number to locate the right routine in the array and invokes it, providing it with the aforementioned input data structure.

In case of a user mode callback, in Pin the registered `CONTEXT_CALLBACK_NOTIFICATION` function is invoked right before `KiUserCallbackDispatcher`'s execution, obviously with the reason paramater set to `CONTEXT_CHANGE_REASON_CALLBACK`.

In light of what just stated, it is natural for BlueTracer's logging activity, taking place in the registered `CONTEXT_CALLBACK_NOTIFICATION` function, to involve the record of a callback occurrence, together with the name of the callback that is about to be invoked. Unfortunately, tracing the callback's arguments would require further work since they are packed in a data structure, as previously explained.

[4] The process environment block (PEB) is a data structure employed in Windows operating systems to represent a user mode process [9]

Right before the execution of `KiUserCallbackDispatcher`, i.e. when the registered `CONTEXT_CALLBACK_NOTIFICATION` function is called, the stack looks as follows (*Figure 3.7*).

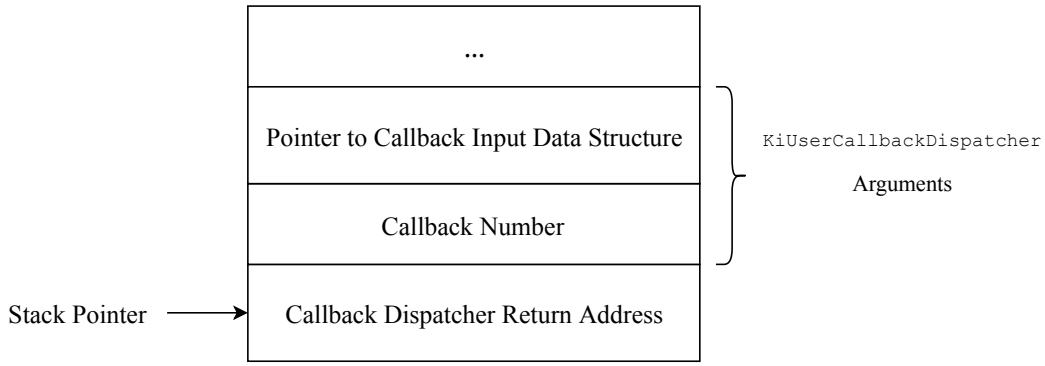

Figure 3.7. *Stack before `KiUserCallbackDispatcher` execution*

Having this in mind, it is now possible to explain step-by-step how the tracing of callbacks takes place in BlueTracer:

1. The stack pointer value is retrieved. This is achieved through the use of the `PIN_GetContextReg` API, that allows to get the value of a register in the context provided as input. Such context, in our specific case, is the application's register state after the context change, which, as previously mentioned, is passed as argument to the `CONTEXT_CHANGE_CALLBACK` notification function.

2. The callback number is obtained by adding 4 to the stack pointer and fetching the pointed value, in accordance to *Figure 3.7*.

3. The `KernelCallbackTable` is retrieved from the PEB.

4. The function pointer stored in the `KernelCallbackTable` entry indicated by the callback number is acquired.

5. It is checked if the address of the function falls within `User32.dll` memory address range. In fact, in `Win32` user mode callbacks are employed exclusively by `User32.dll` for windowing related aspects [2], meaning that the retrieved function address must belong to `User32.dll`'s memory address range. Such range is

determined by retrieving an handle for `User32.dll` through `GetModuleHandle`, building an `IMG` object from it utilizing Pin's `IMG_FindByAddress` and invoking the usual `IMG_LowAddress` and `IMG_HighAddress` functions.

6. The name of the callback is determined by creating a `RTN` object from the function address via `RTN_FindByAddress` and consequently invoking `RTN_Name` on such object.

7. The callback occurrence and the callback name is recorded in the log.

The result of the aforementioned callback tracing procedure is a log entry having the following format (*Listing 3.16*).

```
Context change caused by callback -> USER32.dll!LoadMenuW
```

Listing 3.16. Log entry relative to a user mode callback

3.5.2 Windows Asynchronous Procedure Calls Tracing

Windows Asynchronous Procedure Calls (APCs) are employed to alter a thread's ordinary execution path and reroute it to execute some other code. An important concept related to APCs is that, every time an APC is scheduled, it is intended for a specific thread.

APCs are utilized in many situations. Some examples are:

- The I\O Manager employs an APC to terminate an I\O operation inside the thread which started it.
- There exists a particular APC which is used to forcibly enter in a process' execution when it has to terminate.
- Some APIs, like `ReadFileEx` and `WriteFileEx`, utilize APCs when performing asynchronous I\O operations.

APCs are of different types, one of which is user mode APCs. These usually call user mode code and are normally dispatched when the thread willingly enters into an

alertable state. This means that, typically, user mode APCs do not asynchronously force themselves into the targeted thread, but they can be seen more like a set of work items in a queue, which the thread processes when he decides to do so [24].

Just like `KiUserCallbackDispatcher` for user mode callbacks, APCs are channelled by means of a single dispatcher function inside `ntdll`, named `KiUserApcDispatcher`. Such function receives as input a set of paramaters, including the address of the APC routine to be invoked and the references to two data structures in which the APC's arguments are stored [1].

If a user mode APC takes place, in Pin the registered `CONTEXT_CALLBACK_NOTIFICATION` function is called immediately before the execution of `KiUserApcDispatcher`, with the reason parameter, this time, set to `CONTEXT_CHANGE_REASON_APC`. Therefore, the course of action taken by BlueTracer to record user mode APCs is exactly the same as the ones for user mode callbacks, i.e. tracing the APC occurrence as well as the name of the APC that is about to be executed. Once again, however, BlueTracer does not yet support arguments' tracing in this scenario since, also in this case, the arguments are packed in data structures.

Let us now go through the steps employed by BlueTracer to trace user mode APCs:

1. The stack pointer value is retrieved, exactly in the same way as explained for user mode callbacks in section 3.5.1

2. The address of the APC to be invoked is obtained by adding 4 to the stack pointer and fetching the pointed value. In fact, in the stack, the APC address is located right on top of the APC's dispatcher return address, which is pointed by the stack pointer.

3. Given the address of the APC to be invoked, the corresponding `RTN` object is created via `RTN_FindByAddress`. Similarly, from the APC address, the `IMG` object representing the DLL exporting the APC is also built, this time through the use of `IMG_FindByAddress`.

4. The APC name and the DLL name are determined by invoking `RTN_Name` and `IMG_Name` respectively on the objects created in the previous step.

5. The APC-related data is recorded in the log. This includes the APC occurrence, the name of the DLL exporting the APC and the APC name.

The resulting log format is exactly the same as the one adopted for user mode callbacks (*Listing 3.17*).

```
Context change caused by APC -> ifsutil.dll!?HardRead@IO_DP_DRIVE@@QAEEVBIG_INT@@KPAX@Z
```

Listing 3.17. Log entry relative to a user mode APC

3.6 Conclusions

In this chapter we have provided a detailed description of how BlueTracer was organized and implemented. We have first introduced its building blocks, i.e., the Intel Pin DBI framework and the BluePill anti-evasion software toolkit. We have then showed the tool's architecture, outlining its three core components: the Native API tracer, the API tracer and, the user-mode callbacks and APCs tracer. Next, we have explained how the issues related to multithreading were handled, and, finally, we have thoroughly analyzed each one of three aforementioned elements.

Chapter 4

Experimental Evaluation

In this chapter we will illustrate the results obtained during the experimental evaluation of BlueTracer.

We first tested the tool on a set of benign applications performing different tasks, in order to assess its run-time overhead.

Then, we validated BlueTracer using *Al-Khaser* [3], a popular open-source project employed to assess how stealthy a malware analysis system is with respect to a large portion of public evasion techniques used by real malware families.

All the tests were conducted on a VirtualBox (version 5.2.6) Virtual Machine with 1 CPU core and 3 GB of RAM running Windows 7 32-bit. The specifications of the host machine are:

- **Operating System:** Linux Mint 17.3
- **Processor:** Intel Core i7-3537U CPU @ 2.00 GHz × 2
- **RAM:** 8 GBs

4.1 Run-Time Overhead Assessment

In order to evaluate the run-time overhead introduced by BlueTracer we tested it with a number of benign applications exercising a large number of functions. In order to experiment with a wide range of different functionalities, we picked a set of

well-known Windows applications performing a variety of jobs. We grouped these applications based on the task they carry out, as shown below:

- **Collection of system information**
  - `Systeminfo`. It outputs a summary of OS-environment parameters.
  - `System File Checker (SFC)`. It scans for corruptions in system files.
  - `Check Disk`. It checks the disks' integrity.
  - `IPConfig`. It displays TCP/IP network configuration values.
  - `Netstat`. It can show active TCP connections as well as TCP and UDP ports on which the computer is listening.
  - `Driver Query`. It presents the list of installed drivers and their properties.
  - `Windows Assessment Tools (WinSAT)`. It measures a number of performance characteristics and reports them.
  - `Powercfg`. It enables to search for common energy-efficiency problems.
- **Compression programs**
  - `7zip`.. Its default output extension is `.7z`.
  - `IZArc`. Its default output extension is `.zip`.
  - `WinRar`. Its default output extension is `.rar`.
- **Encryption Utilities**
  - `Cipher`. It uses Encrypting File System (ESF), based on DESX.
  - `OpenSSL`. It was configured to employ 256-bit CBC AES.
  - `Crypt`. It adopts RC2 block encryption.
- **Hashing Utilities**
  - `File Checksum Integrity Verifier (FCIV)`. It was set to use both MD5 and SHA1.
  - `TurboSFV`. It was configured to adopt SHA3-224.

We first recorded the native execution time for each of the aforementioned applications. Then, we ran them under BlueTracer, logging the respective execution times. Specifically, the following BlueTracer modes of operation were employed:

- **Empty Image.** All image notification functions are empty, that is, they just increase a global counter value. This means that no analysis routines are inserted at run-time.
- **Empty Routine.** All analysis routines are empty, i.e., all they do is, once again, increase a global counter value.
- **Main Image.** Only Native APIs and APIs being directly invoked from the main executable of the pinned application are traced. This is BlueTracer's default mode of operation.
- **Complete.** Every event is traced, also including Native APIs and APIs being invoked outside the main executable.

We tested every benign application in the previous page adopting each of the above operation modes, which can be set using BlueTracer's configuration file. Essentially, **Empty Image** and **Empty Routine** were utilized to determine the run-time overhead introduced just by the Pin's framework, when no analysis is actually performed. On the contrary, **Main Image** was adopted to show BlueTracer's overhead during a typical use of the tool, as **Main Image** is BlueTracer's default mode. Lastly, **Complete** was employed to determine how BlueTracer's behaves under heavy stress conditions.

We tested each application three times and then recorded the average execution time. For the compression programs, the file being compressed was the Puppy Linux ISO (`xenialpup-7.5-uefi.iso`), of size 332 MBs. On the other hand, for the encryption and hashing utilities, we used the Ubuntu 18.04 ISO (`ubuntu-18.04-desktop-amd64`), the size of which is 1.8 GBs. During the tests, we also decided to stop the execution of the pinned application if, after it had been running for more than 10 minutes, the log file was greater than 5 GBs. This had to be done due to the hard drive limitations of the testing platform.

The recorded execution times can be observed from *Table 4.1*. As it can be seen, as more demanding modes of operation are employed, the run-time increases, although the increment is not uniform, but is actually quite variable across the different applications.

In light of this, to actually quantify the run-time overhead we decided to adopt the following metric:

$$\text{Overhead per Event} = \frac{T_{instrumented} - T_{native}}{Events}$$

where:

- $T_{instrumented}$ is the application's execution time when executed under BlueTracer with the **Complete** mode of operation enabled. We chose the **Complete** mode of operation to quantify the overhead per event in the worst-case situation.
- T_{native} is the application's native execution time.
- $Events$ is the total number of Native API and API calls performed by the analyzed application.

Table 4.2 lists the overhead per event value of each benign application for which the execution time in the **Complete** mode of operation could be obtained. In this case we can see that the typical overhead is approximately in the 4×10^{-5} - 22×10^{-5} seconds range, with the compression programs being an exception, as they have a greater overhead per event value than the rest.

4.2 Al-Khaser

Al-Khaser [3] is a popular open-source application which performs a large number of common checks employed by malware families to determine if they are being executed in an analysis environment. It is typically utilized to assess how stealthy and well hidden a malware analysis system is. For this reason, we chose Al-Khaser as our main validation tool.

Application	Native (s)	Empty Image (s)	Empty Routine (s)	Main Image (s)	Complete (s)
Systeminfo	5.894	9.686	12.869	15.694	26.398
SFC	218.251	222.065	226.125	230.869	245.476
Check Disk	101.570	171.94	181.429	454.649	600+
IPConfig	0.105	4.257	8.421	9.599	13.181
Netstat	0.085	2.563	4.630	6.902	21.129
DriverQuery	1.168	6.663	9.786	34.074	68.668
WinSat	163.175	212.496	221.012	273.641	600+
PowerCFG	61.333	73.325	80.018	132.466	273.882
7zip	175.526	212.000	225.091	227.985	233.792
IZArc	30.920	52.878	56.631	61.066	65.770
WinRar	155.674	192.638	198.804	208.606	215.455
Cipher	0.028	1.817	3.787	4.435	5.064
OpenSSL	24.769	33.183	34.308	47.006	1524.763
Crypt	65.392	140.048	142.979	572.353	600+
FCIV	10.807	25.113	28.144	56.329	87.948
TurboSFV	34.412	57.705	62.639	66.439	74.657

Table 4.1. Execution times of instrumented benign applications

Application	Native (s)	Complete (s)	Events	Overhead per Event ($10^{-}5$ s)
Systeminfo	5.894	26.398	387 476	5.291
SFC	218.251	245.476	333 781	8.156
IPConfig	0.105	13.181	94 313	13.864
Netstat	0.085	21.129	542 649	3.878
DriverQuery	1.168	68.668	1 735 859	3.860
PowerCFG	61.333	273.882	4 497 247	4.726
7zip	175.526	233.792	146 578	39.751
IZArc	30.920	65.770	109 142	31.931
WinRar	155.674	215.455	84 329	70.890
Cipher	0.028	4.435	24 141	18.255
OpenSSL	24.769	1524.763	57 410 809	2.613
FCIV	10.807	87.948	725 133	10.638
TurboSFV	34.412	74.657	183 455	21.937

Table 4.2. Run-time overhead for benign applications

The checks implemented by Al-Khaser are divided into categories, with the most significant ones being the following:

- **Anti-Debugging**, aimed at detecting the presence of a debugger.
- **Anti-Sandbox Timing-based**, the purpose of which is to let sandboxes time out in order to defy analysis.
- **Human Interaction Detection**, which seek to discover the presence of a sandbox by looking for the lack of human interaction with the system.
- **Anti-Virtualization**, which have the objective of exposing the use of virtualization and full-system emulation.
- **Anti-Analysis**, aimed at uncovering the employment of common analysis tools (e.g OllyDbg, IDA Pro, etc.).

When Al-Khaser's executable is run, all the checks are performed and the outcome of each one of them can be easily observed from the command line: `GOOD` is printed if the analysis product succeeded at remaining hidden, and `BAD` otherwise.

To validate BlueTracer, Al-Khaser was run under it in the default **Main Image** mode. The result was that BlueTracer managed to remain undetected with respect to all the checks performed by Al-Khaser. From this outcome we obtained a first confirmation of BlueTracer's ability to hide its presence.

Furthermore, to also validate BlueTracer's tracing power, we analyzed the logs obtained when running Al-Khaser, with the objective of finding evidence of the performed evasion checks. Even in this case, BlueTracer performed well, as the majority of the checks could easily be deduced from the log file.

Let us now show how some of these checks appeared on the log, in order to give a better idea of what BlueTracer is capable of. To be as clear as possible, we will use the same checks categorization as Al-Khaser's.

4.2.1 Anti-Debugging

Anti-debugging checks are essentially aimed at determining if a program is running under a debugger. As already mentioned in section 2.1.5, there exist Windows APIs

whose objective is exactly to discover if the calling process is being debugged. A well-known API of this kind is `IsDebuggerPresent`, which returns a nonzero value if the calling process is running in the context of a debugger and zero otherwise. Such API is employed in one of Al-Khaser's anti-debugging checks and is appropriately recorded by BlueTracer (*Listing 4.1*). As it can be seen below, the return value is zero, as no debugger is detected.

```
~~3160~~ 562 kernel32.dll!IsDebuggerPresent
~~3160~~ 563 KERNELBASE.dll!IsDebuggerPresent
563    executed KERNELBASE.dll!IsDebuggerPresent =>
563     retval: 0x0 (name=Return value, type=(long/int), size=0x4)
```

Listing 4.1. Log entry relative to `IsDebuggerPresent`

Another popular Windows API for debug detection is `CheckRemoteDebuggerPresent`, which determines if the specified process is being debugged by a "remote" debugger, i.e., a debugger residing in parallel and different process. Its second argument is a pointer to a boolean, which is set to true if the provided process is being debugged, or false otherwise. Al-Khaser also adopts this API, and, again, BlueTracer correctly logged its invocation (*Listing 4.2*). In addition, it is worth noting that the output value for the second argument (`arg 1`) is false (`0x0`), thus showing once more that a debugger was not discovered.

```
~~3160~~ 1450 kernel32.dll!CheckRemoteDebuggerPresent
1450    arg 0: 0xffffffff (name=hProcess, type=DWORD, size=0x4)
1450    arg 1: 0x002bf710 => 0x0 (name=pbDebuggerPresent, type=(long/int)*, size=0x4)
1450    executed kernel32.dll!CheckRemoteDebuggerPresent =>
1450    arg 1: 0x002bf710 => 0x0 (name=pbDebuggerPresent, type=(long/int)*, size=0x4)
1450    retval: 0x1 (name=Return value, type=(long/int), size=0x4)
```

Listing 4.2. Log entry relative to `CheckRemoteDebuggerPresent`

Debugger detection is not only achieved through the use of Windows APIs. In fact, there are also some Native APIs which can be used for this purpose. One of them is `NtQueryInformationProcess`, which retrieves information related to the specified process. Its second parameter is utilized to specify the type of process

information to be retrieved. When set to `ProcessDebugPort` (value `0x7`), the Native API provides information on whether or not the supplied process is being debugged. Specifically, if a debugger is present, the `ProcessInformation` output parameter is set to a non-zero port number, while, if the process is not under a debugger, this parameter is set to zero [32]. Al-Khaser performs this check and, once more, BlueTracer recorded it (*Listing 4.3*). In particular, it can be deduced from `arg 1`'s value that `ProcessDebugPort` is adopted. Unfortunately, this time, we cannot tell from the log that a debugger has not been detected because the output paramater containing this information (`arg 2`) is a pointer to a `struct`, which changes based on the type of process information requested. BlueTracer does not yet address these complex cases and we are planning to address them in future versions of the tool.

```
~~3160~~ 3186 ntdll.dll!NtQueryInformationProcess
3186    arg 0: 0xffffffff (type=HANDLE, size=0x4)
3186    arg 1: 0x7 (type=int, size=0x4)
3186    arg 2: 0x002bf6cc (type=<struct>*, size=0x4)
3186    arg 3: 0x0 (type=unsigned int, size=0x4)
3186    arg 4: 0x003c0e98 (type=unsigned int*, size=0x4)
3186    succeeded =>
3186    arg 2: 0x002bf6cc (type=<struct>*, size=0x4)
3186    arg 4: 0x003c0e98 => 0x3c0ea0 (type=unsigned int*, size=0x4)
3186    retval: 0x0 (type=NTSTATUS, size=0x4
```

Listing 4.3. Log entry relative to `NtQueryInformationProcess`

4.2.2 Anti-Sandbox Timing-based

Anti-sandbox timing-based checks have the objective of hindering dynamic analysis by making sandboxes time out and, in some cases, they also measure the time elapsed between sleep operations to detect time fast-forwarding strategies. Luckily, BluePill [12] addresses these checks by adopting a sophisticated strategy based on manipulating the timer behaviour of a process. This means that BlueTracer can record timing-based checks without worrying about being detected.

The `NtDelayExecution` Native API is lowest level user mode mechanism which

can be employed to suspend execution. It takes as input two paramaters: a boolean that makes the Native API alertable when set to `true` and a `LARGE_INTEGER` defining the delay interval. If the value for the second parameter is negative, it specifies the *relative* amount to sleep in units of 100 nanoseconds; otherwise, it indicates an *absolute time*, i.e. the date and time when to stop sleeping. Al-Khaser makes use of this Native API and BlueTracer was able to correctly trace it (*Listing 4.4*). In particular, from the log entry, it can be seen that a negative delay was specified, meaning that a *relative* time to sleep was provided.

```
~~3160~~ 46332 ntdll.dll!NtDelayExecution
46332   arg 0: 0x0 (type=bool, size=0x1)
46332   arg 1: 0xfffffffff4d2fa200(hex) (type=LARGE_INTEGER*, size=0x4)
46332    succeeded =>
46332   retval: 0x0 (type=NTSTATUS, size=0x4)
```

Listing 4.4. Log entry relative to `NtDelayExecution`

`WaitForSingleObject` is also often used to wait until a time-out interval elapses. In input, it receives an handle to an object and a time-out interval in milliseconds. Then, it waits until the provided object is in the signaled state or the time-out runs out. Al-Khaser also adopts this API in its set of timing-based checks. Once more, BlueTracer was capable of recording its occurrence (*Listing 4.5*). It is relevant to point out that the return value is `0x102`, which indicates that the API has returned because the time-out interval has elapsed, just as expected.

```
~~3160~~ 50077 kernel32.dll!WaitForSingleObject
50077   arg 0: 0x204 (name=hHandle, type=DWORD, size=0x4)
50077   arg 1: 0x493e0 (name=dwMilliseconds, type=DWORD, size=0x4)
50077    executed kernel32.dll!WaitForSingleObject =>
50077   retval: 0x102 (name=Return value, type=DWORD, size=0x4)
```

Listing 4.5. Log entry relative to `WaitForSingleObject`

The most well-known API for suspending execution is surely `sleep`, that simply takes as input the number of milliseconds for which execution is to be delayed. Due to its popularity, Al-Khaser had to adopt it and, again, BlueTracer's logs showed

evidence of its usage (*Listing 4.6*). Specifically, from the log file, it can be deduced that `sleep` was used in a loop, as it is invoked many times subsequently.

```
~~3160~~ 9225 kernel32.dll!Sleep
9225    arg 0: 0xf (name=dwMilliseconds, type=DWORD, size=0x4)
~~3160~~ 9226 KERNELBASE.dll!Sleep
9226    arg 0: 0xf (name=dwMilliseconds, type=DWORD, size=0x4)
9226    executed KERNELBASE.dll!Sleep =>
9226    retval: 0x00000000 (name=Return value, type=void, size=0x0)
~~3160~~ 9227 ntdll.dll!NtYieldExecution
9227    failed (error=0x40000024) =>
9227    retval: 0x40000024 (type=NTSTATUS, size=0x4)
~~3160~~ 9228 kernel32.dll!Sleep
9228    arg 0: 0xf (name=dwMilliseconds, type=DWORD, size=0x4)
~~3160~~ 9229 KERNELBASE.dll!Sleep
9229    arg 0: 0xf (name=dwMilliseconds, type=DWORD, size=0x4)
9229    executed KERNELBASE.dll!Sleep =>
9229    retval: 0x00000000 (name=Return value, type=void, size=0x0)
~~3160~~ 9230 ntdll.dll!NtYieldExecution
9230    failed (error=0x40000024) =>
9230    retval: 0x40000024 (type=NTSTATUS, size=0x4)
```

Listing 4.6. Portion of `Sleep` loop

4.2.3 Human Interaction Detection

The idea behind human interaction detection checks is to uncover the presence of a sandbox based on the lack of human interaction with the system; in fact, in real environments users typically perform some detectable activities when carrying out their tasks. A classical example of such activities is moving the mouse cursor.

The mouse cursor position can be obtained through the use of the `GetCursorPos` API, which has a single output parameter containing a pointer to a `POINT struct`. Such data structure stores the retrieved position of the mouse cursor, in screen coordinates. Al-Khaser employs the `GetCursorPos` API to check if there is some kind of mouse movement in the sandbox. Even in this case, BlueTracer proved to work well as it traced the API's invocation (*Listing 4.7*). It is interesting to

notice that, from the log, it can be also deduced how the actual check is carried out by Al-Khaser. In fact, `GetCursorPos` is called, followed by a `Sleep` and another `GetCursorPos` invocation. In light of this, it is likely that an initial cursor position was first retrieved, which was later compared with the cursor position obtained after the sleep operation, with the aim of determining if the mouse cursor had moved in the mean time.

```
~~3160~~ 17964 USER32.dll!GetCursorPos
17964   arg 0: 0x002bf684 (name=lpPoint, type=struct*|tagPOINT, size=0x40)
17964    executed USER32.dll!GetCursorPos =>
17964   arg 0: 0x002bf684 (name=lpPoint, type=struct*|tagPOINT, size=0x40)
17964   retval: 0x1 (name=Return value, type=(long/int), size=0x4)
~~3160~~ 17965 kernel32.dll!Sleep
17965   arg 0: 0x1388 (name=dwMilliseconds, type=DWORD, size=0x4)
~~3160~~ 17966 KERNELBASE.dll!Sleep
17966   arg 0: 0x1388 (name=dwMilliseconds, type=DWORD, size=0x4)
17966    executed KERNELBASE.dll!Sleep =>
17966   retval: 0x00000000 (name=Return value, type=void, size=0x0)
~~3160~~ 17967 USER32.dll!GetCursorPos
17967   arg 0: 0x002bf698 (name=lpPoint, type=struct*|tagPOINT, size=0x40)
17967    executed USER32.dll!GetCursorPos =>
17967   arg 0: 0x002bf698 (name=lpPoint, type=struct*|tagPOINT, size=0x40)
17967   retval: 0x1 (name=Return value, type=(long/int), size=0x4)
```

Listing 4.7. `GetCursorPos` evidence in the log

4.2.4 Anti-Virtualization

Anti-virtualization checks look for a number of artifacts in the guest operating system introduced by hypervisors which are specific to virtual machines.

A common way to detect virtualization is by checking Windows registry artifacts. The Windows registry is a hierarchical tree-like database containing critical data for both the Windows operating system and its applications. Each node of the tree is a *key* and every key embodies *subkeys* and *values* [35]. The existence of some specific registry keys is enough to reveal the presence of virtualization. For instance, the key `HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX\__` gives away the presence

of VirtualBox. Al-Khaser looks for these kinds of Windows registry artifacts and BlueTracer is able to record such events (*Listing 4.8*). From the listing below, it can be observed that the aforementioned registry key is searched through the use of the `RegOpenKeyExW` API, which normally opens the specified registry key. However, in this case, a file not found error value (`0x2`) is returned since the registry key is not found, thus also confirming BlueTracer's ability to remain hidden.

```
~~3160~~ 30134 ADVAPI32.dll!RegOpenKeyExW
30134   arg 0: 0x80000002 (name=hKey, type=DWORD, size=0x4)
30134   arg 1: HARDWARE\ACPI\DSDT\VBOX__ (name=lpSubKey, type=wchar_t*, size=0x2)
30134   arg 2: 0x0 (name=ulOptions, type=DWORD, size=0x4)
30134   arg 3: 0x20019 (name=samDesired, type=DWORD, size=0x4)
30134   arg 4: 0x002bf6e4 => 0x0 (name=phkResult, type=DWORD*, size=0x4)
~~3160~~ 30135 kernel32.dll!RegOpenKeyExW
30135   arg 0: 0x80000002 (name=hKey, type=DWORD, size=0x4)
30135   arg 1: HARDWARE\ACPI\DSDT\VBOX__ (name=lpSubKey, type=wchar_t*, size=0x2)
30135   arg 2: 0x0 (name=ulOptions, type=DWORD, size=0x4)
30135   arg 3: 0x20019 (name=samDesired, type=DWORD, size=0x4)
30135   arg 4: 0x002bf6e4 => 0x0 (name=phkResult, type=DWORD*, size=0x4)
30135    executed kernel32.dll!RegOpenKeyExW =>
30135   arg 4: 0x002bf6e4 => 0x0 (name=phkResult, type=DWORD*, size=0x4)
30135   retval: 0x2 (name=Return value, type=(long/int), size=0x4))
```

Listing 4.8. Log entry relative to `RegOpenKeyExW`

In addition to Windows registry artifacts, there are also many file system artifacts which can be checked in order to uncover the presence of a virtualized environment. Typically, specific files are searched. Al-Khaser, for instance, looks for a number of files, one of which is the `VboxMouse.sys` driver of Virtualbox. Once more, BlueTracer was able to trace these file-searching events, including the ones relative to `VboxMouse.sys` (*Listing 4.9*). The `GetFileAttributesW` API, as the name suggests, is typically employed to obtain file attributes for the specified file. From *Listing 4.9* it can be seen that the API returns -1, since the requested file was not found. Therefore, even in this situation, BlueTracer was also undetected.

```
~~3160~~ 24979 kernel32.dll!GetFileAttributesW
24979   arg 0: C:\Windows\system32\drivers\VBoxMouse.sys
 (name=lpFileName, type=wchar_t*, size=0x2)
~~3160~~ 24980 KERNELBASE.dll!GetFileAttributesW
24980   arg 0: C:\Windows\system32\drivers\VBoxMouse.sys
 (name=lpFileName, type=wchar_t*, size=0x2)
24980    executed KERNELBASE.dll!GetFileAttributesW =>
24980   retval: 0xffffffff (name=Return value, type=DWORD, size=0x4)
```

Listing 4.9. Log portion relative to the search for `VboxMouse.sys` search

A virtualized environment can be also discovered by looking for specific windows. The `FindWindow` API returns an handle of a window belonging to a specific class or having the specified name. This API can be exploited to check for the presence of a window associated to a virtualization program. A typical example of this trick, which is implemented by Al-Khaser, is searching for a window named "VBoxTrayToolWnd", as the presence of such window indicates that VirtualBox is being utilized. BlueTracer also detected this check (*Listing 4.10*). As it can be seen, the return value is `null`, meaning that the window was not found and that BlueTracer did not reveal its presence.

```
~~3160~~ 35247 USER32.dll!FindWindowW
35247   arg 0: <null> (name=lpClassName, type=wchar_t*, size=0x2)
35247   arg 1: VBoxTrayToolWnd (name=lpWindowName, type=wchar_t*, size=0x2)
35247    executed USER32.dll!FindWindowW =>
35247   retval: 0x0 (name=Return value, type=DWORD, size=0x4)
```

Listing 4.10. Log entry relative to `FindWindowW`

4.2.5 Anti-Analysis

Lastly, anti-analysis checks are aimed at detecting the existence processes belonging to popular analysis tools. One of such tools is Process Monitor (`procmon.exe`), which is an advanced Windows monitoring tool that shows real-time file system, registry and process/thread activity [29]. Al-Khaser looks for the processes of many analysis tools, including the process associated to Process Monitor. Again, BlueTracer was

also able to successfully log anti-analysis events, even the ones directed at uncovering the presence of Process Monitor (*Listing 4.11*). From the listing below, it can be seen that the course of action adopted by Al-Khaser is quite straightforward. It first takes a snapshot of all the processes in the system with `CreateToolhelp32Snapshot`. Then, for each process in the snapshot, it retrieves the corresponding name, through the use of `Process32FirstW` at the beginning and `Process32NextW` afterwards, and compares it with `procmon.exe` via `StrCmpIW`.

```
~~3160~~ 53940 kernel32.dll!CreateToolhelp32Snapshot
53940   arg 0: 0x2 (name=dwFlags, type=DWORD, size=0x4)
53940   arg 1: 0x0 (name=th32ProcessID, type=DWORD, size=0x4)
53940    executed kernel32.dll!CreateToolhelp32Snapshot =>
53940   retval: 0x1fc (name=Return value, type=DWORD, size=0x4)
~~3160~~ 53941 kernel32.dll!Process32FirstW
53941   arg 0: 0x1fc (name=hSnapshot, type=DWORD, size=0x4)
53941   arg 1: 0x002b7408 (name=lppe, type=struct*|tagPROCESSENTRY32W, size=0x1160)
53941    executed kernel32.dll!Process32FirstW =>
53941   arg 1: 0x002b7408 (name=lppe, type=struct*|tagPROCESSENTRY32W, size=0x1160)
53941   retval: 0x1 (name=Return value, type=(long/int), size=0x4)
~~3160~~ 53942 SHLWAPI.dll!StrCmpIW
53942   arg 0: [System Process] (name=psz1, type=wchar_t*, size=0x2)
53942   arg 1: procmon.exe (name=psz2, type=wchar_t*, size=0x2)
53942    executed SHLWAPI.dll!StrCmpIW =>
53942   retval: 0xffffffff (name=Return value, type=(long/int), size=0x4)
~~3160~~ 53943 kernel32.dll!Process32NextW
53943   arg 0: 0x1fc (name=hSnapshot, type=DWORD, size=0x4)
53943   arg 1: 0x002b7408 (name=lppe, type=struct*|tagPROCESSENTRY32W, size=0x1160)
53943    executed kernel32.dll!Process32NextW =>
53943   arg 1: 0x002b7408 (name=lppe, type=struct*|tagPROCESSENTRY32W, size=0x1160)
53943   retval: 0x1 (name=Return value, type=(long/int), size=0x4)
~~3160~~ 53944 SHLWAPI.dll!StrCmpIW
53944   arg 0: System (name=psz1, type=wchar_t*, size=0x2)
53944   arg 1: procmon.exe (name=psz2, type=wchar_t*, size=0x2)
53944    executed SHLWAPI.dll!StrCmpIW =>
53944   retval: 0x1 (name=Return value, type=(long/int), size=0x4)
```

Listing 4.11. `procmon.exe` search

4.3 Conclusions

In this chapter we have outlined the results of BlueTracer's experimental evaluation. In order to assess BlueTracer's run-time overhead, we have tested it on a number of applications performing various tasks, employing a four different modes of operation. We have also introduced the overhead per event metric as a way of quantifying the run-time overhead introduced by BlueTracer. The results showed that the typical overhead per event is in the 4×10^{-5} - 22×10^{-5} seconds range. Then we validated BlueTracer with Al-Khaser, an open-source application employed to assess how stealthy an analysis system is with respect to many evasion techniques used in the wild. BlueTracer was able to remain hidden to all the checks performed by Al-Khaser, thus proving to be effective at staying undetected. Furthermore, BlueTracer's tracking abilities also turned out to be efficacious, since evidence of the vast majority of Al-Khaser's techniques was present in BlueTracer's log.

Chapter 5

Conclusions

Donec et nisl id sapien blandit mattis. Aenean dictum odio sit amet risus. Morbi purus. Nulla a est sit amet purus venenatis iaculis. Vivamus viverra purus vel magna. Donec in justo sed odio malesuada dapibus. Nunc ultrices aliquam nunc. Vivamus facilisis pellentesque velit. Nulla nunc velit, vulputate dapibus, vulputate id, mattis ac, justo. Nam mattis elit dapibus purus. Quisque enim risus, congue non, elementum ut, mattis quis, sem. Quisque elit.

5.1 Future Directions

Two areas:

1. Tools capabilities: support for struct, compatibility extension, more malwares tested

2. Data Analysis Techniques: data analysis for threat intelligence to analyze the logs.

Bibliography

[1] *A catalog of NTDLL kernel mode to user mode callbacks, part 3: KiUserApcDispatcher*. 2007. URL: http://www.nynaeve.net/?p=202.

[2] *A catalog of NTDLL kernel mode to user mode callbacks, part 5: KiUserCallbackDispatcher*. 2007. URL: http://www.nynaeve.net/?p=204.

[3] *Al-Khaser v0.74*. 2018. URL: https://github.com/LordNoteworthy/al-khaser.

[4] P. Arafa, H. Kashif, and S. Fischmeister. "DIME: Time-aware dynamic binary instrumentation using rate-based resource allocation". In: *2013 Proceedings of the International Conference on Embedded Software (EMSOFT)*. 2013, pp. 1–10. DOI: 10.1109/EMSOFT.2013.6658603.

[5] Ulrich Bayer and Christopher Krügel. "TTAnalyze : A Tool for Analyzing Malware". In: 2005.

[6] J. Berdajs and Z. Bosnić. "Extending Applications Using an Advanced Approach to DLL Injection and API Hooking". In: *Softw. Pract. Exper.* 40.7 (June 2010), pp. 567–584. ISSN: 0038-0644. DOI: 10.1002/spe.v40:7. URL: http://dx.doi.org/10.1002/spe.v40:7.

[7] Armin Buescher, Felix Leder, and Thomas Siebert. "Banksafe Information Stealer Detection Inside the Web Browser". In: *Proceedings of the 14th International Conference on Recent Advances in Intrusion Detection*. RAID'11. Menlo Park, CA: Springer-Verlag, 2011, pp. 262–280. ISBN: 978-3-642-23643-3. DOI: 10.1007/978-3-642-23644-0_14. URL: http://dx.doi.org/10.1007/978-3-642-23644-0_14.

[8] Geoff Chappell. *Native API Functions*. 2017. URL: https://www.geoffchappell.com/studies/windows/win32/ntdll/api/native.htm.

[9] Geoff Chappell. *PEB*. 2016. URL: https://www.geoffchappell.com/studies/windows/win32/ntdll/structs/peb/index.htm.

[10] *Chapter 1: Introduction to Win32/Win64*. 2018. URL: https://technet.microsoft.com/en-us/library/bb496995.aspx.

[11] *Cisco 2018 Annual Cybersecurity Report*. 2018. URL: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf.

[12] Daniele Cono D'Elia et al. *The DBI Blue Pill: Practical Analysis of Evasive Malware*. Technical report, currently under double-blind review at ACM ACSAC. 2018.

[13] *Deviare API Hook Overview*. 2012. URL: https://www.nektra.com/products/deviare-api-hook-windows/.

[14] *Dr.Memory*. URL: http://drmemory.org/.

[15] *Dynamic Binary Instrumentation*. 2007. URL: http://uninformed.org/index.cgi?v=7&a=1&p=3.

[16] *Dynamic Instrumentation Tool Platform*. URL: http://www.dynamorio.org/.

[17] *Dynamic-Link Libraries*. 2018. URL: https://msdn.microsoft.com/en-us/library/windows/desktop/ms682589(v=vs.85).aspx.

[18] Manuel Egele et al. "A Survey on Automated Dynamic Malware-analysis Techniques and Tools". In: *ACM Comput. Surv.* 44.2 (Mar. 2008), 6:1–6:42. ISSN: 0360-0300. DOI: 10.1145/2089125.2089126.

[19] *Intercepting all System Calls by Hooking KiFastSystemCall*. 2015. URL: https://www.malwaretech.com/2015/04/intercepting-all-system-calls-by.html.

[20] *Internet Security Threat Report, vol. 23*. 2018. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

[21] Ivo Ivanov. *API hooking revealed*. 2002. URL: https://www.codeproject.com/Articles/2082/API-hooking-revealed.

[22] Chi-Keung Luk et al. “Pin: Building Customized Program Analysis Tools with Dynamic Instrumentation”. In: *Proceedings of the 2005 ACM SIGPLAN Conference on Programming Language Design and Implementation*. PLDI ’05. ACM, 2005. DOI: 10.1145/1065010.1065034.

[23] Tarjei Mandt. *Kernel Attacks through User-Mode Callbacks*. URL: https://media.blackhat.com/bh-us-11/Mandt/BH_US_11_Mandt_win32k_WP.pdf.

[24] Enrico Martignetti. *Windows Vista APC Internals*. 2009. URL: http://www.opening-windows.com/download/apcinternals/2009-05/windows_vista_apc_internals.pdf.

[25] Syed Zainudeen Mohd Shaid and Mohd Maarof. “In memory detection of Windows API call hooking technique”. In: (Aug. 2015), pp. 294–298.

[26] Nicholas Nethercote. “- CL-TR-606 ISSN 1476-2986 Dynamic binary analysis and instrumentation”. In: 2004.

[27] *Pin - A Dynamic Binary Instrumentation Tool*. 2012. URL: https://software.intel.com/en-us/articles/pin-a-dynamic-binary-instrumentation-tool.

[28] Mario Polino et al. “Measuring and Defeating Anti-Instrumentation-Equipped Malware”. In: *Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA)*. Bonn, Germany, 2017.

[29] *Process Monitor v3.50*. 2018. URL: https://docs.microsoft.com/en-us/sysinternals/downloads/procmon.

[30] *PyREbox*. 2018. URL: https://talosintelligence.com/pyrebox.

[31] Mark Russinovich. *Inside the Native API*. 1998. URL: http://persephone.cps.unizar.es/~spd/pub/windows/ntdll.htm.

[32] Michael Sikorski and Andrew Honig. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*. 1st. San Francisco, CA, USA: No Starch Press, 2012. ISBN: 1593272901, 9781593272906.

[33] A. Skaletsky et al. "Dynamic program analysis of Microsoft Windows applications". In: *2010 IEEE International Symposium on Performance Analysis of Systems Software (ISPASS)*. 2010, pp. 2–12. DOI: 10.1109/ISPASS.2010.5452079.

[34] Sherri Sparks, Shawn Embleton, and Cliff C. Zou. "WINDOWS ROOTKITS A GAME OF HIDE AND SEEK". In: *Handbook of Security and Networks*. 2011, pp. 345–368. DOI: 10.1142/9789814273046_0014. eprint: https://www.worldscientific.com/doi/pdf/10.1142/9789814273046_0014. URL: https://www.worldscientific.com/doi/abs/10.1142/9789814273046_0014.

[35] *Structure of the Registry*. 2018. URL: https://docs.microsoft.com/en-us/windows/desktop/sysinfo/structure-of-the-registry.

[36] Dafydd Stuttard et al. *Attack and Defend Computer Security Set*. 1st. Wiley Publishing, 2014. ISBN: 111890673X, 9781118906736.