7J-04

UEFIと64bit環境のためのマルウェア動的解析システムAlkanet

中山 崇嗣 † 金城 聖 † 毛利 公一 †
† 立命館大学情報理工学部

1 はじめに

近年，マルウェアの数は亜種の登場により増加が著しい [1]．マルウェアによる被害を防ぐためにはマルウェアの特徴を調査する必要があるが，マルウェアの数の増加もあって調査には時間をかけることができない．そうした中で，マルウェアを静的解析することは，膨大なマルウェアの数に対して時間がかかりすぎるため，動的解析を活用することが時間短縮に寄与する．一方で，マルウェアの中には動的解析が行われる仮想環境を検知して動作を変えるものや，解析を回避するものが存在する [2]．こうした問題を解決すべく，我々はマルウェアに仮想環境の存在を検知させることなく，システムコールをトレースすることで動的解析を行うAlkanet[3] を開発してきた．

マルウェアの攻撃対象となる環境は，レガシーBIOSや32bit OSを搭載した計算機環境からUEFI BIOSや64bit OSを搭載した計算機環境へと変化している．こうしたマルウェアの動作環境の変化に合わせてマルウェアの解析環境を更新することは重要であり，古い解析環境のままではマルウェアに対処できない．本論文では，近年主流となっているUEFI BIOSと64bit Windows環境を対象に64bitマルウェアの解析をするため，AlkanetをUEFI BIOS環境に対応させ，64bitマルウェアを解析し動作を確認したので報告する．

2 システムコールトレーサ Alkanet

本章ではAlkanetの概要について述べる．その後，AlkanetのUEFI BIOSと64bit OSへの対応について述べる．

2.1 概要

AlkanetはハイパーバイザであるBitVisor[4]の拡張機能として実装された．BitVisorは多くのI/Oをパススルーする準パススルー型のハイパーバイザであり，デバイスをゲストOSが制御する特徴をもつ．そのため，複数のゲストOSを動作させるために必要な仮想化されたデバイスから，仮想環境特有の実機には存在しない特徴をマルウェアに検知されない．AlkanetではBitVisor上でWindowsにおけるシステムコールをトレースすることで，マルウェアから検知されにくい高速な動的解析環境を実現している．

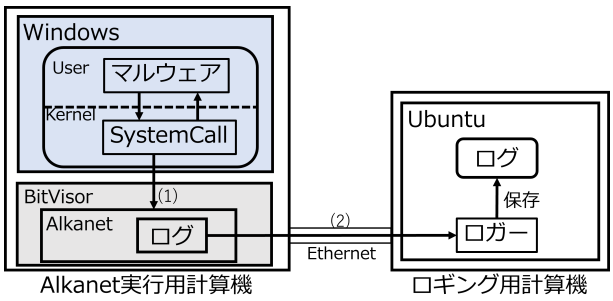

図1 Alkanetの構成図

Alkanetの構成を図1に示す．Alkanetでは2台の計算機を用いて解析する．Alkanet実行用計算機では(1)に示すように，Windowsの全プロセスを対象に発行されたシステムコールを実行時と終了時でそれぞれフックする．フック時にはシステムコールの発行元プロセス名や引数，戻り値などの情報も合わせて取得し，ロギング用計算機に送信する．ロギング用計算機ではAlkanetの制御とAlkanet実行用計算機から送信される(2)のログを受信する．

2.2 UEFI BIOSのための Alkanet 更新

AlkanetのベースとなるBitVisorをUEFI BIOSをサポートしたものに更新することで，AlkanetをUEFI BIOSからのブート可能とし，同環境でのトレースを実現した．Alkanetがシステムコールをトレースする流れを示す．

1. プロセスがシステムコールを発行
2. ハードウェアブレイクによりデバッグ例外が発生
3. BitVisorが例外をトラップ
4. システムコールトレース

AlkanetのベースとなるBitVisorの更新のためには，新たなBitVisorにAlkanetの機能追加のための改変が必要になる．BitVisor上でAlkanetが動作するために必要な改変を以下に示す．

- システムコールフックのための MSR(Model-specific register) の設定
- フック時にAlkanetへ遷移する処理の追加

Malware Dynamic Analysis System Alkanet for UEFI and 64-bit Environments
Takatsugu Nakayama†, Akira Kanashiro†, and Koichi Mouri†
†College of Information Science and Engineering, Ritsumeikan Univ.

表 1　Alkanet 実行用計算機環境

CPU	Intel Core i7-8700
メモリ	32GB
BIOS	UEFI BIOS
Guest OS	64bit 版 Windows 10 Version 1909

表 2　使用したマルウェア

ファイル名	Akrien.exe
ハッシュ値 (SHA-1)	377e21f001fa53e3cf1d 5a1f8738442ba78721ab
ファイル形式	PE32+
ファイルサイズ	7.66MB

フックポイントを追加するための MSR の設定と例外発生時の処理は BitVisor から提供される API を通して行われる．BitVisor が UEFI BIOS をサポートするために行われた改変は BitVisor 起動時の処理であり，Alkanet の実装に必要な BitVisor の API に大きな影響はない．そのため，Alkanet への影響が最小限になる BitVisor を選定したうえで，Alkanet の再実装に必要な 352 行の改変を加え Alkanet の処理をマージすることで Alkanet を更新した．

3　動作検証

本章では，実際のマルウェアを用いて Alkanet が UEFI BIOS を搭載した計算機上で 64bit マルウェアを解析する動作検証をした．マルウェアを VirusTotal[5] から取得し，Alkanet の解析結果が VirusTotal 上で公開されているマルウェアの活動一致するか比較することで検証した．

3.1　検証環境

使用した Alkanet の実行環境を表 1 に示す．Alkanet が 64bit マルウェアを解析可能であることを示すため，UEFI BIOS を搭載した計算機上で 64bit マルウェアを解析した．

3.2　マルウェアを用いた検証

VirusTotal で公開されている 64bit マルウェアを Alkanet で解析することで動作検証をした．使用したマルウェアを表 2 に示す．Akrien.exe は 71 のセキュリティベンダ中 49 ベンダが悪意のあるファイルであると判断したマルウェアである．

表 2 の Akrien.exe は実行後，インストーラが古い旨の書かれたロシア語のポップアップを表示した後に終了した．Alkanet はマルウェアの呼び出したシステムコールのうち，27 種についてトレースした．その中でマルウェアの呼び出した NtCreateFile システムコールの一部を図 2 に示す．図 2 では NtCreateFile のプロセス名やファイルのアクセス権が desired_access から確認できる．また，ファイルパスとして C:\Windows\Globalization\Sorting\sortdefault.nls が指定されていることも確認できる．

```
"no": 654311,
"cpu_id": 0,
"logtype": "ENTER",
"proc_pid": "21f4",
"proc_tid": "21f8",
"proc_name": "7d317343ffac1b",
"name": "NtCreateFile",
"sys_no": "55",
"type": "syscall",
(中略)
"ret_val": "0",
"additional_info": {
    "desired_access": "80100080",
    "file_name": "0\\\\??\\C:\\Windows\\
      Globalization\\Sorting\\sortdefault.nls"
}
```

図 2　Alkanet の解析ログ

今回マルウェアとして実行した Akrien.exe は sortdefault.nls 以外にも NtCreateFile の引数として C:\Windows\AppPatch\sysmain.sdb が渡されるファイルアクセスを観測した．この 2 つのファイル作成は VirusTotal でも報告されている挙動であることから，Alkanet は UEFI BIOS と 64bit OS の環境上で 64bit マルウェアを解析可能であると判断できる．

4　おわりに

本稿では UEFI BIOS と 64bit OS の環境上で動作するマルウェアに対応するため，Alkanet を UEFI BIOS に対応させ，マルウェアを解析することで Alkanet が UEFI BIOS を搭載した計算機上で動作することを示した．今後は WSL 上で動作するマルウェアやファイルレスマルウェアに対して Alkanet を用いて解析する予定である．

参考文献

[1] G DATA Software AG: G DATA Malware Report H2 2014, https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/GData_PCMWR_H2_2014_EN_v1.pdf (2014).

[2] Afianian, A., Niksefat, S., Sadeghiyan, B. and Baptiste, D.: Malware Dynamic Analysis Evasion Techniques: A Survey, *ACM Comput. Surv.*, Vol. 52, No. 6 (2019).

[3] 大月勇人，瀧本栄二，齋藤彰一，毛利公一：マルウェア観測のための仮想計算機モニタを用いたシステムコールトレース手法，情報処理学会論文誌，Vol. 55, No. 9, pp. 2034–2046 (2014).

[4] Shinagawa, T., Eiraku, H., Tanimoto, K. et al.: BitVisor: A Thin Hypervisor for Enforcing i/o Device Security, *Proceedings of the 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments*, New York, NY, USA, Association for Computing Machinery, p. 121–130 (2009).

[5] VirusTotal: https://www.virustotal.com.