

Static Malware Analysis Dan Implementasi Sigma & Yara Rules



ID-Networkers
Indonesian IT Expert Factory



Note:

This Report Is Based On My Experience And Point Of View As A Beginner, Thankyou

Nama Peserta : Raja Ubaid Fawwaz

Username : Raja x NG / NewbieGanas

A. Penjelasan

1. Malware

Malware adalah singkatan dari malicious software, artinya, program yang diciptakan khusus untuk menyusup ke dalam sebuah sistem tanpa sepengetahuan pemiliknya dan bertahan di sana untuk jangka waktu tertentu. Biasanya, malware menyamar sebagai program yang tidak berbahaya untuk mengelabui pengguna.

Dampak dari perangkat lunak berbahaya ini jauh lebih serius bagi perusahaan dibandingkan pengguna perorangan. Serangan malware pada sistem jaringan perusahaan bisa menyebabkan kerusakan dan gangguan yang luas, membutuhkan upaya pemulihan yang besar di seluruh organisasi.

2. Sigma Rules

Sigma adalah Generic Signature Format for SIEM Systems yang berarti sebuah format khusus yang bisa digunakan atau dikonversikan oleh banyak SIEM yang ada secara generic. Tujuannya adalah agar sebuah aturan deteksi cukup dibuat sekali dalam format Sigma, lalu bisa secara otomatis diterjemahkan ke dalam berbagai bahasa query yang spesifik untuk setiap platform SIEM (Security Information and Event Management).

3. Yara Rules

YARA merupakan singkatan dari Yet Another Recursive Acronym atau Yet Another Ridiculous Acronym berupa tools yang bersifat Open Source yang dibuat oleh Victor Alvarez dari VirusTotal. YARA digunakan untuk mengidentifikasi dan mengklasifikasikan malware melalui penggunaan aturan berbasis signature dan karakteristik target lainnya yang dapat dijalankan pengguna terhadap file dan YARA rules yang lebih maju, seperti mencari data di alamat virtual memory tertentu dalam proses yang sedang berjalan.



B. Implementasi

1. Malware Analysis Result

- Lab01-01.exe

The screenshot shows the VirusTotal analysis interface for the file Lab01-01.exe. The file has a Community Score of 55/72 and is flagged as malicious by 55/72 security vendors. The file size is 16.00 KB and it was last analyzed 19 hours ago. The file type is Win32 EXE. The basic properties section lists various hashes and file information.

Property	Value
MD5	bb7425b82141a1c07d60e5106676bb1
SHA-1	9dce39ac1bd36d877fdb0025ee88daff0627cdb
SHA-256	58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47
Vhash	014036151d1bza0fz
Authenticash	094eed7cfc959fd9ba704d5fe0b965b7bb6ca09d302870935dc0508d940ba2c
Imphash	2b5f75aa75c57ed7c68f7be490d63605
Rich PE header hash	6a52cc2e068dfb8f2b4715556fd89a66
SSDEEP	96:1t6Y5CuDzp17S5eVIV2cFL+31zrx9+NNoy:nv6V7117S5ercZ+FznxcNNoy
TLSH	T17C72B44376E51CB1EF2811B6429293FC927DE0604766F2EE78731A46D432893793CADB
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (console) Intel 80386, for MS Windows
TrID	Microsoft Visual C++ compiled executable (generic) (38.4%) Win32 Dynamic Link Library (generic) (15.3%) Win16 NE executable (generic) (11.7%) Win32 Executable ...
DetectItEasy	PE32 Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] Compiler: Microsoft Visual C/C++ (12.00.8168) [C++] Linker: Microsoft Linker (6.00.8168) Tool: ...
Magika	PEBIN
File size	16.00 KB (16384 bytes)
PEID packer	Microsoft Visual C++

Merupakan Malware yang menjadi eksekutor file .dll dengan nama yang sama (Lab01-01.dll). dilihat dari fungsi import pada KERNEL32.dll seperti **FindNextFile**, **CopyFile**, **FindFirstFile**. Malware ini bisa mencari file yang menjadi pasangannya dan mengeksekusinya

Malware Ini Dicompile Pada 2010-12-19 16:16:19 UTC



- Lab01-01.dll

The image shows a VirusShare analysis page for a file named 'Lab01-01.dll'. At the top, a red circle indicates a 'Community Score' of 46 out of 71. A red banner states '46/71 security vendors flagged this file as malicious'. The file's SHA-256 hash is 'f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba'. The file size is 160.00 KB, and it was last analyzed 2 days ago. Below the header, there are tabs for 'DETECTION', 'DETAILS', 'RELATIONS', 'BEHAVIOR', and 'COMMUNITY'. The 'DETAILS' tab is selected, showing 'Basic properties'. The properties list includes MD5, SHA-1, SHA-256, Vhash, Authentihash, Imphash, Rich PE header hash, SSDEEP, TLSH, File type (Win32 DLL), Magic (PE32 executable (DLL) (GUI) Intel 80386, for MS Windows), TrID (Win32 Dynamic Link Library (generic) (27.1%), Win16 NE executable (generic) (20.8%), Win32 Executable (generic) (18.6%), Windows Icons Library (generic) (8.5%), ...), DetectItEasy (PE32), Compiler (EP:Microsoft Visual C/C++ (6.0 (1720-8966)) [DLL32]), Linker (Microsoft Visual C/C++ (12.00.8168) [C++] [Tool: ...]), Magika (PEBIN), File size (160.00 KB (163840 bytes)), and PEID packer (Microsoft Visual C++ v6.0 DLL).

Merupakan pasangan dari malware Lab01-01.exe tadi. Karena file .dll tidak bisa berjalan sendiri. Dilihat dari fungsi import pada KERNEL32.dll yaitu **CreateMutex**, **CreateProcessA**, **Sleep**. Dan WS2_32.dll yaitu **socket**, **closesocket**, **inet_addr** dan **connect** dapat diasumsikan bahwa pasangan malware ini bisa berkomunikasi dengan server eksternal untuk melakukan Command and Control

Malware Ini Dicompile Pada : 2010-12-19 16:16:38 UTC

Pasangan Malware Ini Menargetkan Sistem Windows, namun dilihat dari waktu compilenya sepertinya windows versi lama. Namun tidak menutup kemungkinan bisa menargetkan versi terbaru



- Lab01-02.bin

The image shows a VirusTotal analysis of a file named 'Lab01-02.bin'. The file is 3.00 KB and was last analyzed 2 days ago. It is marked as 'EXE'. The analysis shows that 57 out of 71 security vendors flagged this file as malicious. The file's SHA-1 hash is 5a016facbcb77e2009a01ea5c67b39af209c3fcb. The file type is Win32 EXE, and it is identified as a PE32 executable (console) Intel 80386, for MS Windows, UPX compressed. The file is packed with UPX v0.89.6 - v1.02 / v1.05 - v1.24 -> Markus & Laszlo [overlay]. The file is also identified as a Packer: UPX (3.04) [NRV,best]. The file is also identified as a Compiler: Microsoft Visual C/C++ (12.00.8168) [C++]. The file is also identified as a Linker: Microsoft Linker (6.00.8168). The file is also identified as a Tool: Visual Studio (6.0).

Property	Value
MD5	8363436878404da0ae3e46991e355b83
SHA-1	5a016facbcb77e2009a01ea5c67b39af209c3fcb
SHA-256	c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6
Vhash	03303e0f7d10192601pz1bz
Authenticity hash	c0dd97382560a28cc053de86b9505ea78390147de7021744eb49d9b55e3d152f
Imphash	096aa05b8a2e1f2dc66fc73a1a978a7b
Rich PE header hash	0560c88b0c8133e98d13ab271ab4c687
SSDEEP	48:atUKzRhVtNZEVtbn4m3ZUJSSeJY8JTalLoBgs:0UKXktf4KOJzcK
TLSH	T18351B8ABFE665CFAC24E0B3DB9C920356EA0D04BFD43C16A9D7497E89B1548855610
File type	Win32 EXE (executable) windows win32 pe peexe
Magic	PE32 executable (console) Intel 80386, for MS Windows, UPX compressed
TrID	UPX compressed Win32 Executable (34.7%) Win32 EXE Yoda's Crypter (34.1%) Win32 Dynamic Link Library (generic) (8.4%) Win16 NE executable (generic) (6.4%) ...
DetectItEasy	PE32 Packer: UPX (3.04) [NRV,best] Compiler: Microsoft Visual C/C++ (12.00.8168) [C++] Linker: Microsoft Linker (6.00.8168) Tool: Visual Studio (6.0)
Magika	PEBIN
File size	3.00 KB (3072 bytes)
PEID packer	UPX v0.89.6 - v1.02 / v1.05 - v1.24 -> Markus & Laszlo [overlay]
F-PROT packer	UPX

Malware ini dipacked dengan upx, setelah di-unpacked dengan command upx di cmd windows fungsi import melalui beberapa file .dll dan strings yang terbaca di file ini terlihat seperti mencari sebuah service dengan nama MalService dan malware ini kuat dugaannya memiliki hubungan dengan web [http://www.malwareanalysisbook\(.\).com](http://www.malwareanalysisbook(.).com). Malware ini juga bisa berkomunikasi melalui internet dibuktikan dengan fungsi import pada WININET.dll yaitu **InternetOpenUrl** dan **InternetOpen**

Malware Ini Dicompile Pada 2011-01-19 16:10:41 UTC
Dan masih menargetkan sistem windows



2. Sigma Rules Creation

```
Sigconverter
title: Malware Detection
id: 5fe6a618-c510-40bb-b94b-47db34f4e026
status: experimental
description: Detects if a three specific file has been opened or running in the windows system
references:
  - https://medium.com/@Architekt.exe/writing-your-first-sigma-rule-5ed783c87570
  - Noctra Lupra Community
author: Raja x NewbieGanas
date: 2025-07-24
logsource:
  category: file_event
  product: windows
Look Up
detection:
  selection:
    Hashes|contains:
      - 'sha256=58898bd42c5bd3bf9b1389f0eee5b39cd59180e8370eb9ea838a0b327bd6fe47' # Lab01-01.exe
      - 'sha256=f50e42c8dfaab649bde0398867e930b86c2a599e8db83b8260393082268f2dba' # Lab01-01.dll
      - 'sha256=c876a332d7dd8da331cb8eee7ab7bf32752834d4b2b54eaa362674a2a48f64a6' # Lab01-02.bin
    condition: selection
falsepositives:
  - hash value of the file is different either manipulated or the has been rebuild with some manipulation
level: high
```

Sigma rules yang akan saya buat akan mendeteksi kalau file dengan value hash sesuai yang ada di rules dibuka/berjalan. Saya membuatnya seperti ini untuk meminimalisir terjadinya false positive dan langsung spesifik mengarah ke file tertentu saja



3. Yara Rules Creation

Berikut rules yang saya buat

```
// Combo Lab01-01

rule Malware_TwoStage_Backdoor_Lab01_01
{
    meta:
        description = "Detect two specific file which identified as a malware"
        author      = "Raja x NewbieGanas"
        date        = "2025-07-24"
        reference    = "Noctra Lupra Community, Gemini AI"

    strings:
        // String .exe
        $loader_mutex = "WARNING_THIS_WILL_DESTROY_YOUR_MACHINE"
        $loader_dll_typo = "kerne132.dll" ascii

        // String .dll
        $payload_mutex = "SADFHUHF" ascii
        $payload_ip = "127.26.152.13" ascii

    condition:
        uint16(0) == 0x5a4d and
        (
            ($loader_mutex and $loader_dll_typo)
            or
            ($payload_mutex and $payload_ip)
        )
}
```

Konsepnya sederhana, rulesnya akan mendeteksi file yang didalamnya terdapat strings khusus yang diduga mengakibatkan eksploitasi. Namun tidak semua saya input karena akan memicu banyak false positive. Sedangkan bagian condition akan terpenuhi jika file yang dideteksi merupakan file windows dan strings yang dideteksi sama dengan file yang discan, scopenya dipersempit lagi dengan mendeteksi IP spesifik yang menjadi dugaan Server C2 pada malware ini



```
// Lab01-02

rule Malware_Packed_Service_Lab01_02
{
    meta:
        description = "Detect a suspicious file which is identified as a malware"
        author      = "Raja x NewbieGanas"
        date        = "2025-07-24"
        reference    = "Noctra Lupra Community, Gemini AI"

    strings:
        // Indikator Packer UPX
        $upx1 = "UPX0" ascii
        $upx2 = "UPX!" ascii

        // Indikator Behavior
        $behavior_service = "MalService" ascii
        $behavior_mutex   = "SHGL345" ascii
        $behavior_url      = "wareanalysisbook.com" ascii
        $behavior_useragent = "Int6net Explo!r 8FEI" ascii

    condition:
        uint16(0) == 0x5a4d and
        all of ($upx*) and
        2 of ($behavior_*)
}
```

Konsepnya sama seperti sebelumnya perbedaannya ada penambahan deteksi strings UPX karena malware ini dipacked menggunakan upx

Penulisan 2 rules diatas bisa langsung digabung menjadi 1 dokumen



4. Validating The Rules

Untuk sigma rules, saya menggunakan sigma-cli untuk mendeteksi apakah ada kesalahan dalam penulisan rulanya, sigma-cli saya sertakan di bagian referensi

```
(kali㉿kali)-[~/Downloads]
└─$ sigma-cli check sigmaboy.yaml
Parsing Sigma rules [#####] 100%
Checking Sigma rules [#####] 100%

=== Summary ===
Found 0 errors, 0 condition errors and 0 issues.
No rule errors found.
No condition errors found.
No validation issues found.
```

Dan untuk yara rules, kali linux saya sudah terdapat command yara yang bisa digunakan, saya menaruh 3 file malware diatas di dalam satu folder dengan susunan seperti ini

- /Downloads
- Yaraohyara.yaml (yara rules yang dibuat)
 - /Malware
 - Lab01-01.exe
 - Lab01-01.dll
 - Lab01-02.bin

Dan saya menginput command yang hasilnya menunjukan kalau 3 filenya sudah terdeteksi

```
(kali㉿kali)-[~/Downloads]
└─$ yara yaraohyara.yar Malware
Malware_TwoStage_Backdoor_Lab01_01 Malware/Lab01-01.exe
Malware_Packed_Service_Lab01_02 Malware/Lab01-02.bin
Malware_TwoStage_Backdoor_Lab01_01 Malware/Lab01-01.dll
```



5. Reference

<https://www.jaiminton.com/Tutorials/PracticalMalwareAnalysis/Chapter1/>

<https://medium.com/@Architekt.exe/writing-your-first-sigma-rule-5ed783c87570>

<https://github.com/SigmaHQ/sigma-cli>