

# Collecting Malware in Swiss German University with Low Energy and Cost Computer

**Mario Marcello**

Department of Information Technology, Swiss German University, Tangerang 15143, Indonesia

## Article Information

Received: 2 July 2018  
Accepted: 2 August 2018  
Published: 3 October 2018  
DOI: 10.33555/ejaict.v5i2.57

## Corresponding Author:

Mario Marcello  
Email:

ISSN 2355-1771

## ABSTRACT

*The malware spreads massively in Indonesia. The security in Information Technology doesn't seem to become a top priority for Indonesian. The use of pirated software is still high, although it is the biggest threat and entrance for the malwares to attacks. This paper shows how to collect a spreading malware in a system to know the malware trends that exist. So, the owner may know the malware trends inside his system and he can countermeasure the attacks. To collect the malwares, I use the Dionaea, the honeypot to collect malware and implement it to Raspberry Pi. Raspberry Pi is a small, low cost and low energy consumption computer. By using Raspberry Pi to collect malware, we can minimize budget, save the energy and space.*

Keywords: *Dionaea, Honeypot, Raspberry Pi, Malware*

## 1. Introduction

In a survey by KTPG Luxembourg, they state that although industries nowadays already bonded with information technology, industries in 2013 only spend less than 25% of their budget for information technology. And the budget for information security is either remains the same or decreased from 2012 (Hoffman, M., Luxembourg, C.J., 2013). This shows that the industries do not realize about how important the information security is.

In a research from gocsi.com, malware attacks is the number one threats to information security (67% in 2010 and still increasing) (CSI Survey, 2010). That's why an information system needs a device to detect, report, and collect malware. A Honeynet project community has a tool called Dionaea to collect malware. Dionaea is capable to detect and collect malware, even an unknown malware. Dionaea's source code is available online which mean everybody can build/compile the code to any operating system (Dionaea).

To run Dionaea, it does not need to use sophisticated and brand new hardware, even old Pentium can run Dionaea (Spitzner, L. et al., 2004). Currently, there is a micro computer called Raspberry Pi which use ARM processor and it runs Linux. A set of Raspberry Pi cost only ¼ of nanoPC that available in the market. This leads me to use Raspberry Pi as a device to detect and collect malwares.

## 2. Dionaea

Dionaea is a tool from honeynet project community. Dionaea was started by Markus Koetter and it is an open source project, so Dionaea is still developed until now. Basically, Dionaea open seven well-known ports as a trap for attacker (especially malware). It opens FTP, TFTP, HTTP, SMB, MSSQL, MySQL, and VoIP (SIP). When an attack detected, it emulates a fake system and check a file (if any) with libemu to detect whether the file is malicious. When libemu detect anomaly from the file, Dionaea will copy the file to a folder. Dionaea also records the connection information like source IP, source port, date and time to SQLite database. Dionaea must be installed in a special computer that has no any valuable data and different from production computer.

Dionaea can be supported by virustotal. Virustotal is an online malware analysis tools, it cooperates with 51 antivirus vendors to analyze what kind of malware that is uploaded (Virustotal). Dionaea can automatically upload the captured suspicious file to virustotal.

Beside records the connection information, with a help from third party application called p0f (p0f v3), Dionaea can passively detect the operating system that the attackers use. So we may know the statistic of operating system that attackers use.

## 3. Raspberry Pi

Raspberry Pi is a small computer, a credit card sized computer. It consumes maximum for only 5 watts of electricity power. Raspberry Pi has 2 types, type A and B. Type B's specification is higher than type A. This research is using Raspberry Pi type B. Here is the specification of Raspberry Pi type B:

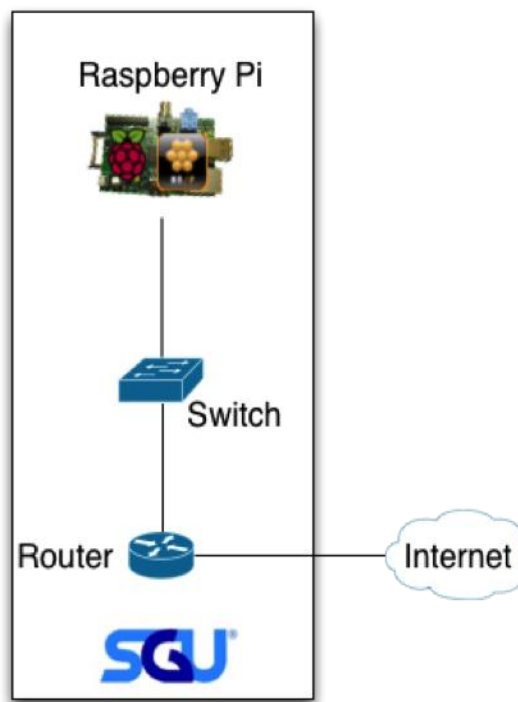
**Table 1.** Raspberry Pi's type B specification.

SoC:	Broadcom BCM2835
CPU:	700MHz ARM1176JZF-S core
GPU:	Broadcom VideoCore IV, OpenGL ES 2.0, OpenVG 1080p30 H.264 high-profile encode/decode
Memory (SDRAM):	512MB (shared with GPU) as of 15 October 2012
USB 2.0 ports:	2
Video outputs:	Composite RCA, HDMI
Audio outputs:	3.5mm jack, HDMI
Onboard storage:	Secure Digital
Onboard network:	10/100 wired Ethernet RJ45
Power ratings:	700mA (3.5W)
Power source:	5 volt via MicroUSB or GPIO header
Size:	85.60mm × 53.98mm
Weight:	45g
Supported Operating systems:	Arch Linux ARM, Debian Linux, Fedora, FreeBSD, Plan 9, Raspbian OS (Debian), RISC OS, Slackware Linux

With the usage of Raspberry Pi, it is effective and efficient in term of electricity, space, and cost compare to normal computer of even nanoPC that exist in the market. Raspberry Pi only consumes 5 watts of electricity power, has the same size of credit card, and has price only  $\frac{1}{4}$  of normal computer.

#### 4. Proposed Architecture

Raspberry Pi with Dionaea is set in Swiss German University. Swiss German University has a block of IP public, which is accessible from anywhere. In order to get attacks, the Raspberry Pi is connected to one IP public. This IP public will not be filtered by any firewall, so any connection is permitted to the honeypot (Dionaea) in Raspberry Pi. Figure 1 shows the proposed architecture to implement Dionaea in Swiss German University.



**Figure 1.** Proposed Architecture for Dionaea implementation in Raspberry Pi.

The operating system for Raspberry Pi is Raspbian, Raspbian is actually a Debian with modification from Raspberry Pi community, so it is developed to make the hardware and operating system compatible each other.

#### 5. Result & Discussion

##### 5.1. Install Dionaea in Raspberry Pi

Dionaea can be installed in Raspberry Pi. It needs some dependencies that can be downloaded, compiled, and installed on Linux operating system. Since the Raspberry Pi runs Raspbian that based on Linux Debian, all dependencies of Dionaea is running well. These are the list of Dionaea's dependencies:

- Libev
- Libglib
- Libssl
- Liblcfg
- Libemu
- Python
- Cython
- Libudns
- Libcurl
- Libpcap
- Libnl
- Libgc

If the dependencies have been installed properly, Dionaea is ready to be installed. The Dionaea's source code can be downloaded from github. Then compiled and installed to the Raspberry Pi. Some modification to Dionaea's configuration must be done to enable automatic virustotal analysis, enable p0f passive OS fingerprinting, and configure logging system to make it efficient.

## 5.2. Capture Result

Dionaea assumes any coming connection as a malicious connection. This is because there must be no normal people want to connect to Dionaea, since it has no valuable data in it. So, any coming connection to Dionaea will be recorded to the SQLite database and Dionaea may also detect any suspicious malware attack. The copies of malware binaries are copied to a folder inside Raspberry Pi.

I started to run Dionaea in Raspberry Pi from March 3<sup>rd</sup> 2014 at 1pm until April 2<sup>nd</sup> 2014 at 5am. In 30 days, Dionaea has captured total 60930 connections. I can obtain the number from the SQLite query:

```
select count(*) from connections;
```

From 60930, there are only 3 captured unique malwares. This might be the same malware attack repeatedly.

```
select virustotalscan_result from virustotals as v, virustotalscans as vs where
v.virustotal=vs.virustotal and vs.virustotalscan_scanner='McAfee';
```

Since I have enabled the automatic malware submission to virustotal, I can see what kind of malware that attacked to the system. Virustotal has cooperated with more than 50 antivirus provider, I obtain the malware's name from McAfee. The SQLite query to obtain them is: The result of the query will be:

The result of the query will be:

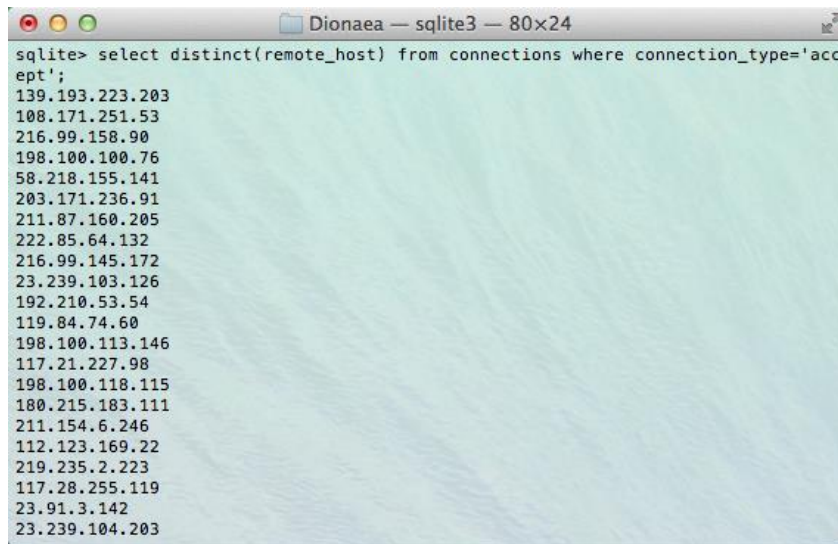
'None' in the query result indicates that McAfee doesn't know what kind of malware it is, or I may say that 'None' means new kind of malware.

```

W32/Conficker.worm.gen.a
W32/Blaster.worm.e
None

```

And the most important in capture result is the attacker's IP address. We may see all the IP addresses that come to Dionaea. Here is the query:



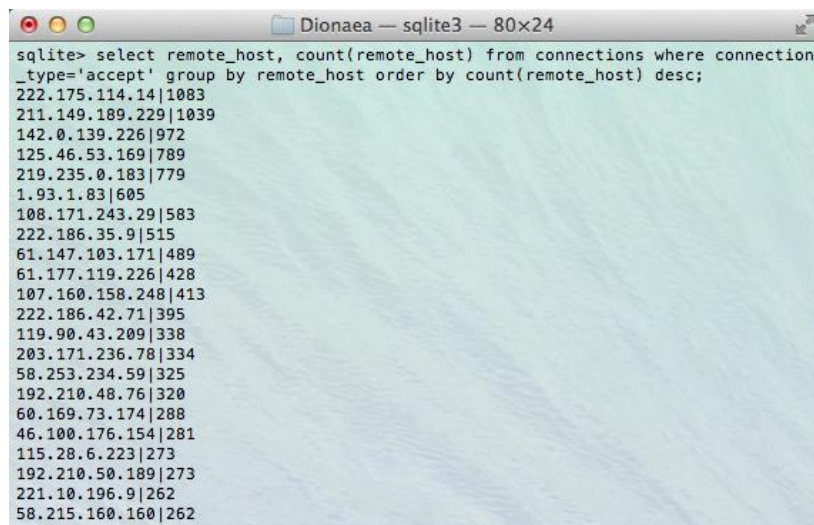
```

Dionaea — sqlite3 — 80x24
sqlite> select distinct(remote_host) from connections where connection_type='accept';
139.193.223.203
108.171.251.53
216.99.158.90
198.100.100.76
58.218.155.141
203.171.236.91
211.87.160.205
222.85.64.132
216.99.145.172
23.239.103.126
192.210.53.54
119.84.74.60
198.100.113.146
117.21.227.98
198.100.118.115
180.215.183.111
211.154.6.246
112.123.169.22
219.235.2.223
117.28.255.119
23.91.3.142
23.239.104.203

```

**Figure 1** The query of unique attacker's IP address

Or, we may see the frequency of attacker come to Dionaea:



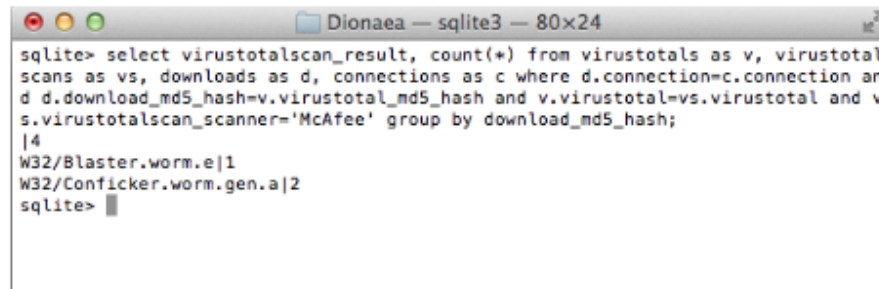
```

Dionaea — sqlite3 — 80x24
sqlite> select remote_host, count(remote_host) from connections where connection_type='accept' group by remote_host order by count(remote_host) desc;
222.175.114.14|1083
211.149.189.229|1039
142.0.139.226|972
125.46.53.169|789
219.235.0.183|779
1.93.1.83|605
108.171.243.29|583
222.186.35.9|515
61.147.103.171|489
61.177.119.226|428
107.160.158.248|413
222.186.42.71|395
119.90.43.209|338
203.171.236.78|334
58.253.234.59|325
192.210.48.76|320
60.169.73.174|288
46.100.176.154|281
115.28.6.223|273
192.210.50.189|273
221.10.196.9|262
58.215.160.160|262

```

**Figure 2.** Frequency of Attacker.

Besides the frequency of attacker, we may also see the frequency of malware attacks. Here is the query:



```

sqlite> select virustotal_scan_result, count(*) from virustotal
scans as vs, downloads as d, connections as c where d.connection=c.connection an
d d.download_md5_hash=v.virustotal_md5_hash and v.virustotal=vs.virustotal and v
s.virustotal_scanner='McAfee' group by download_md5_hash;
|4
W32/Blaster.worm.e|1
W32/Conficker.worm.gen.a|2
sqlite>

```

It shows that 'None' malware attacked 4 times, W32/Blaster.worm.e once, and W32/Conficker.worm.gen.a twice. From this result we can see that not all coming connections contain malwares and from the result we may obtain the malware attacks trends to the SGU information system.

## 6. Conclusion

Raspberry Pi is capable to be used as malware collector. In order to collect malware, I used Dionaea, the honeypot to capture malware. Dionaea can be installed and run in Raspberry Pi. Raspberry Pi was chosen because it has small size, low energy consumption, low cost, and yet powerful to run Dionaea. Low energy consumption and low cost for information security for an information system in a company might be a solution for the system administrator to obtain the malware attack trends. The malware attack trends can be used as early warning to a company.

## Reference

CSI Survey (2010). Available online: <http://gocsi.com/survey>

Dionaea - catches the bug. Available online: <http://dionaea.carnivore.it>

Hoffman, M., Luxembourg, C.J. (2013). IT security survey 2012-2013. KPMG Luxembourg.

p0f v3. Available online: <http://lcamtuf.coredump.cx/p0f3>

Spitzner, L. et al. (2004). Know Your Enemy: Learning About Security Threats. second edition. Pearson Education.

Virustotal – Free Online virus, malware, and URL scanner. Available online: <http://www.virustotal.com>