

# MyKotakPasir

Automated Binary Analysis

Malware Research Centre, MyCERT



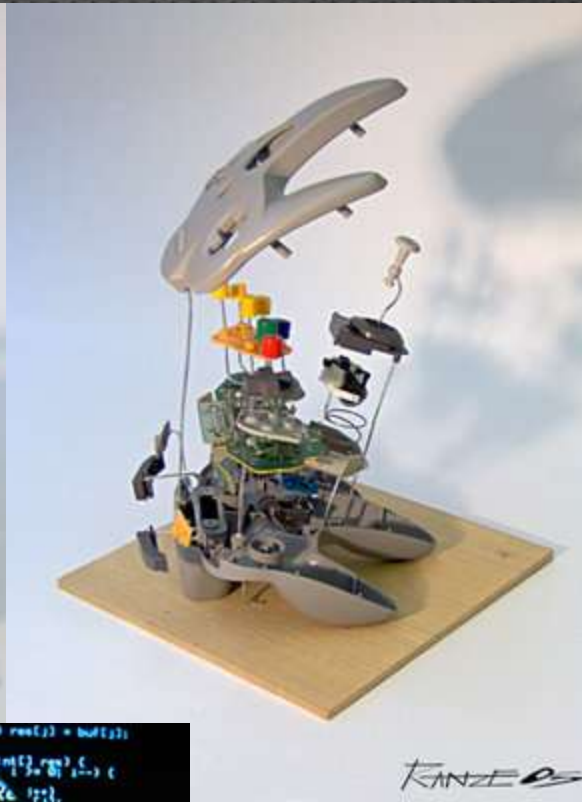
# Agenda

---

- History
- The New MyKotakPasir
- Web User Interfaces
- How it Works
- Where is the URL?
- Limitation
- Other Malware Sandbox
- Future Implementation

# Introduction

- Also known as Automated Malware Analysis or Malware Sandbox
- Help malware analyst to save their time.
- Use sandbox for baseline analysis, and analyst can do static analysis for further info
- Programmed using PHP, Python, MS Visual Basic, C++



```
for (int i = 0; i < len; i++) res[i] = buf[i];
return res;

uint8_t * decodeMessage(uint8_t * res) {
    int i = 0;
    while (i < MAX_RES_LEN) {
        if (buf[i] == 0) {
            res[i] = checkRe[buf[i]];
            i++;
        } else {
            res[i] = buf[i];
            i++;
        }
    }
    return res;
}

uint8_t * extractMessage(uint8_t * res) {
    int i = 0;
    while (i < MAX_RES_LEN) {
        if (buf[i] == 0) {
            res[i] = buf[i];
            i++;
        } else {
            res[i] = buf[i];
            i++;
        }
    }
    return res;
}
```

# History

- Simple Web user interfaces
- For internal use only
- Take more time to analyze the sample
- Based on external tools
- Unmanaged source code, unstable, not optimized
- A lot of weakness
  - Weak password, pcap file reveal internal data, shell upload.



Submit  
Search  
Report

Home

Search For  
» Advanced

Name

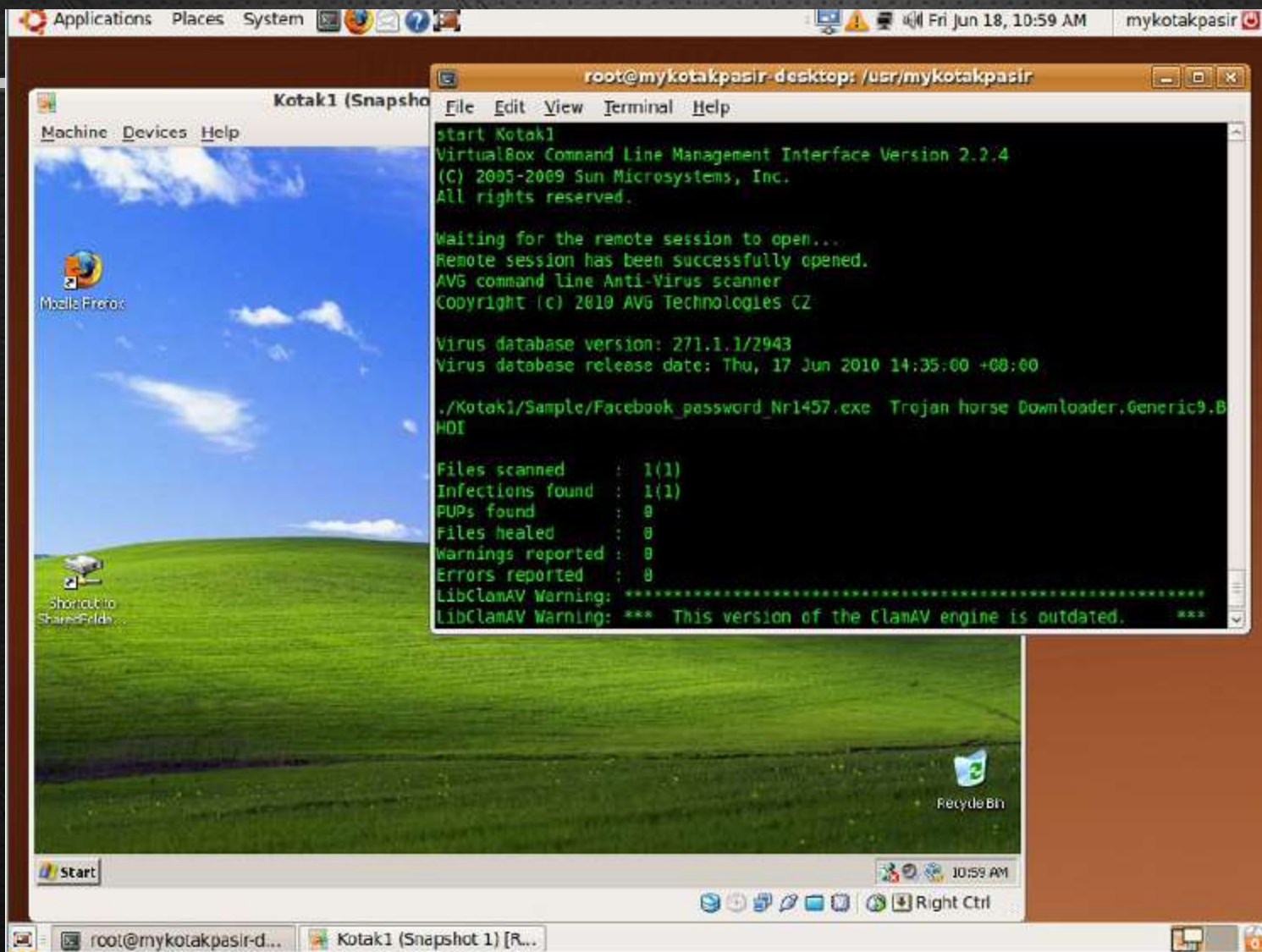
- 93094c
- df07c6f
- b64ca8
- 7b4adc
- 917ae8
- c4e13b

MyKotakPasir Report:

General information	
File Name:	c:\1.exe
MDS:	bbaf9721534391f3a4c87165e992cfc8
SHA-1:	5618d009f94d75b156b974ac6edcde9d69cc9c37
File Size:	363389 Bytes
Packed:	Zip Sfx Archive
PCap File:	<a href="#">Download</a>

- Antivirus Detection	
AVG:	Found Nothing
F-Prot:	Found Nothing
Avast:	Found Nothing
BitDefender:	Dropped:Generic.Malware.Sldd!.F979711F
ClamAV:	Found Nothing

- + File Identifier
- + String Found
- + New Process Run
- + File And Folder Activity
- + NetWork Activity



# Current Implementations

---

- One of 2010 Project
- More stable, less time to analyze
- The URL open to public access
- Report produced more detailed result
- New improved Web UI for easy access
- Require user registration for account management




# Current Implementations

---

- Secured web access
- User can edit their result
- User statistics
- World map Malware plotting
- User Profile
- User have their own web preferences
- Improved search result

MyKotakPasir

https://mykotakpasir.honeynet.org.my



## Login into your account

Username:

Password:

[Forgot your password?](#)



Welcome pentadbir!

Here the list of the latest submission submitted by you.

No	Date	From	Hashes	Comments	Menu
1	2011-08-18 00:02:37	<input type="checkbox"/>	(Suspicious)-DNAScan, WS.Reputation.1, W..	DeBank	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	2011-08-04 23:06:45	<input type="checkbox"/>	Not available	CodeTransport	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	2011-08-04 23:06:45	<input type="checkbox"/>	Not available	Not available.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	2011-08-02 21:52:39	<input type="checkbox"/>	PUA.Tool.RemoveWGA, Trojan.Win32.Genome...	WGA Remover.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5	2011-08-02 21:52:39	<input checked="" type="checkbox"/>	PUA.Tool.RemoveWGA, Trojan.Win32.Genome...	RemoveWGA	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6	2011-08-02 21:30:57	<input type="checkbox"/>	Not available	Not available.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7	2011-08-02 20:50:10	<input type="checkbox"/>	Not available	Not available.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
8	2011-08-02 20:33:35	<input type="checkbox"/>	Not available	Not available.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
9	2011-08-01 23:56:29	<input type="checkbox"/>	Not available	Bkav	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
10	2011-08-01 23:56:29	<input type="checkbox"/>	Not available	Bkav	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
11	2011-08-01 22:11:30	<input type="checkbox"/>	Trojan/W32.Agent.94208.ER, Generic.dxlq..	Adobe Fireworks CS4 Keyg...	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
12	2011-08-01 22:11:30	<input checked="" type="checkbox"/>	Trojan/W32.Agent.94208.ER, Generic.dxlq..	adobe keygen	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
13	2011-07-29 03:40:44	<input type="checkbox"/>	SuspiciousFile, PUA.Packed.PECompact-1, ..	test	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
14	2011-07-26 03:37:12	<input type="checkbox"/>	Not available	Asdasdasdasd	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
15	2011-07-26 03:31:27	<input type="checkbox"/>	Not available	htib bin	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
16	2011-07-26 01:59:46	<input type="checkbox"/>	Not available	Not available.	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
17	2011-07-15 03:49:04	<input type="checkbox"/>	Not available	Hack Hound Crypter	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
18	2011-07-15 03:49:04	<input type="checkbox"/>	Not available	Hack hound	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>



Welcome pentadbir!

Sample Strings Disassembly Screenshot Reanalyze

Submission Details

File Details

Date received: August 18 2011 04:02:33
File Size: 804864 bytes
MD5: 539bc6962479b7bed83ee55e0bf7e9ab
SHA1: afbce998df2fba7a0807e0072db5879f7aa03177
SHA256: a71cc9beccecl0e55431a466ab8a41328503e83ea0a6aa6a543ce74bce5d3e11
Ssdeep: 12288:DYRmMhS9rQKUTrLcepQmZemMWrdAZ0T28QiSNentbKpZ/Ghbe9Dj9kYfwolIEf8:YfstRUPA4RaZ0TjQ5YwwxADuYfwolFi
Compiler: Found nothing.

System Affected

Microsoft Windows XP (32/64 bit), Microsoft Windows Vista (32/64 bit), Microsoft Windows 7 (32/64 bit)

Known Alias

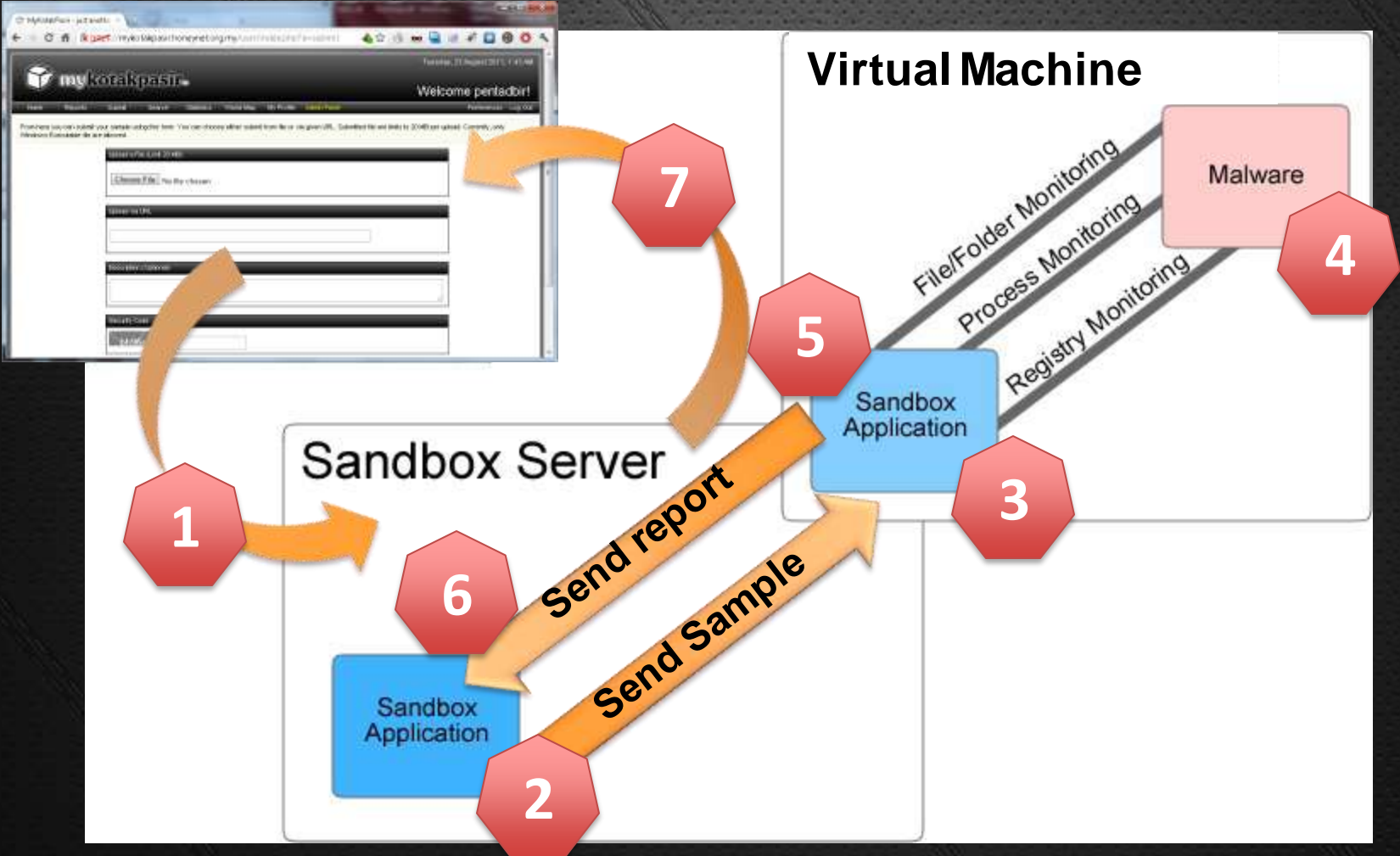
(Suspicious)-DNAScan, WS.Reputation.1, Win32.GenHeur.RP.Xcw, TR/Spy.804864.1,
We have detected 4 out of 43 antivirus engine based on VirusTotal.com services.

File Structures / Advanced File Info

Warning

Suspicious flags set for section 4. Both IMAGE\_SCN\_MEM\_WRITE and IMAGE\_SCN\_MEM\_EXECUTE are set.

# How it works?



# Public Access URL



<https://mykotakpasir.honeynet.org.my>

# Limitation

- Some malware have unique stealth technique.
- Currently we do not provide any Web API for mass upload.
- We cannot guaranteed that our services can provide fast enough to see the result.

# Other Malware Sandbox

- GFI CWSandbox (Sunbelt CWSandbox)
- ThreatExpert
- Joe Sandbox (formerly Joebox)
- Anubis
- Norman Sandbox



# Next Iteration

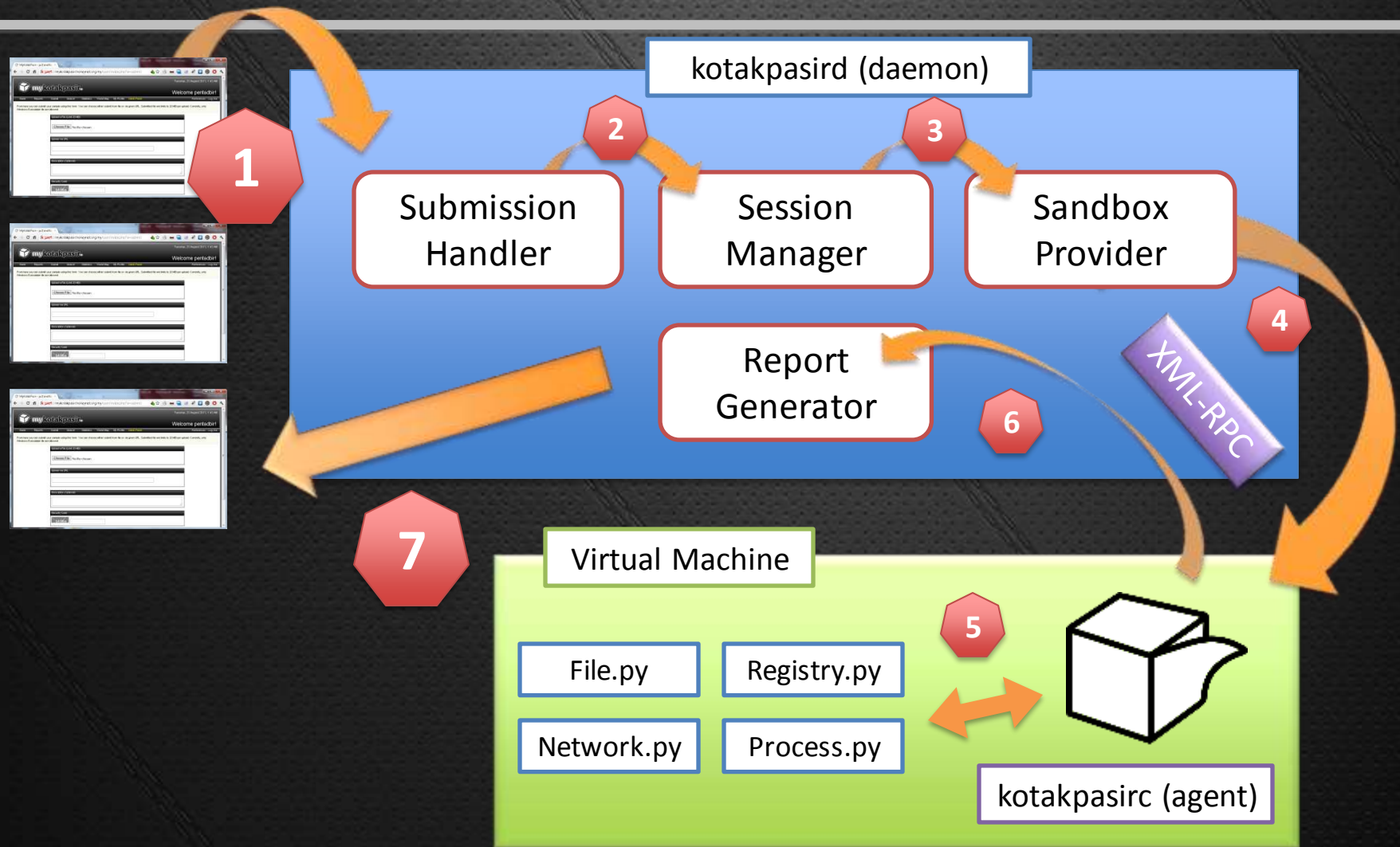
---

- Going framework, going modular
- Modularize everything for flexibility
- Potential integration with other services
- Scale for parallel analysis
- More opportunity to experiment

# Next Iteration

- Python + Django as backend
- “Daemonized” django to serve as the master controller
  - WSGI running in daemon mode
- Why not PHP and cronjobs?
  - Do the right thing
  - Not exactly efficient
  - Troublesome to maintain states

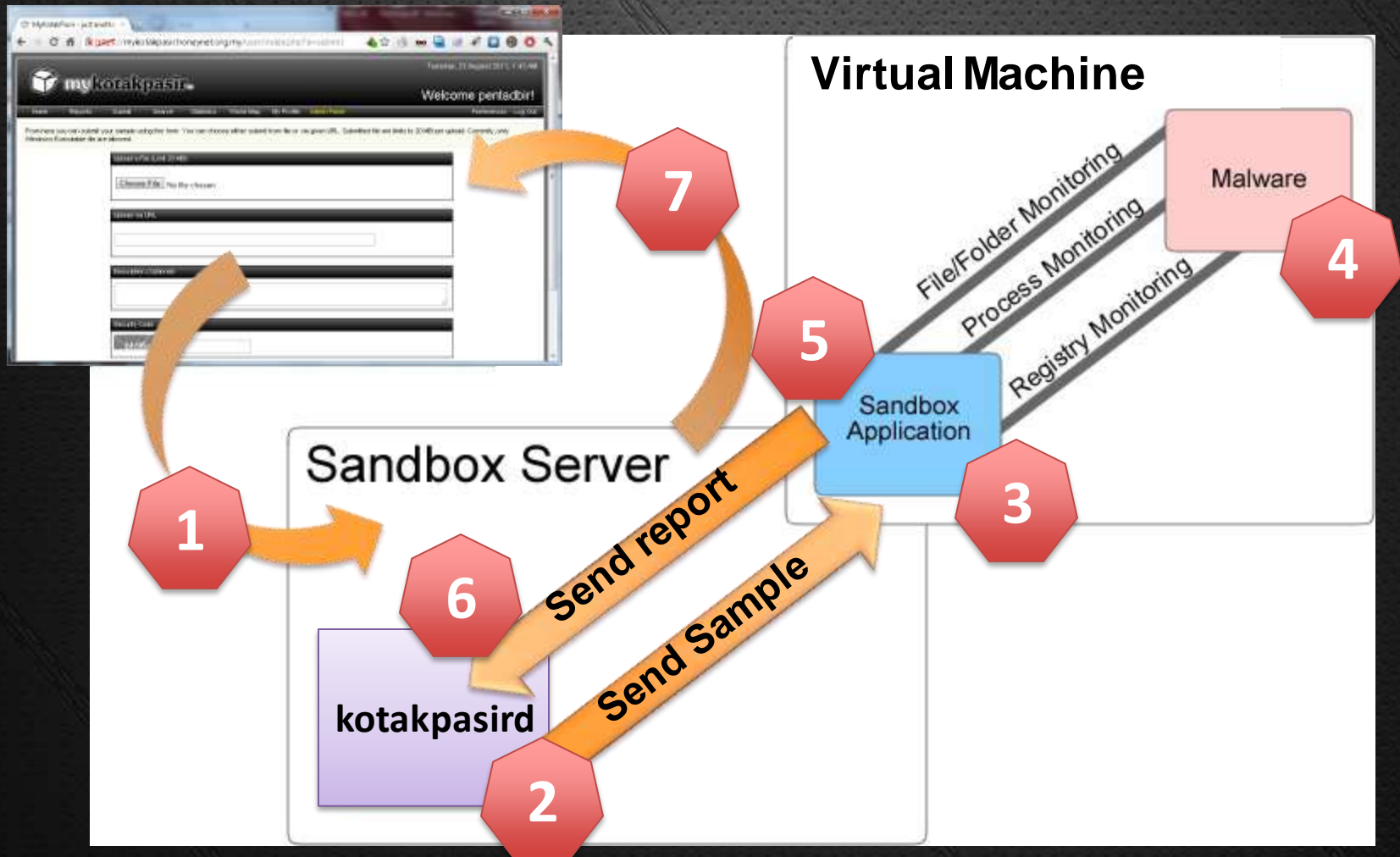
# The Big Picture



# Our Work So Far

- Basic core daemon prototype
- Partially replaced previously poll-driven session manager
- “Backport” the daemon to fit in old system
  - Proof of concept for modularity of new design
  - Reuse previous web interface
  - Convenient unit test

# Our Work So Far



# Expected Improvements

---

- Parallel analysis
  - Handle more sample in shorter time period
  - Spread the analysis load across multiple servers
- Integration
  - API to perform automated submission and analysis
- Hack friendly
  - Write less code to experiment
  - “Battery included”

# Expected Improvements

- Multi sandbox engine support
  - Analysis in multiple environment
    - Observe if malware might behave differently on different platform
    - Eg. Windows XP, Windows 7 64-bit
  - Specialized analysis engine
    - Targets .Net and Java malwares
  - “Timewarp” analysis
    - Observe if malware might behave differently on different date/time
    - “Fast forward” the VM clock 1 week/month/year in advance
  - Any radical ideas you might think of :)

# Conclusion

---

- Save a lot of time to analyze the malware and its behaviour
- Report generated in readable format.
- Easy to manage your own malware analysis result.
- Cost saving

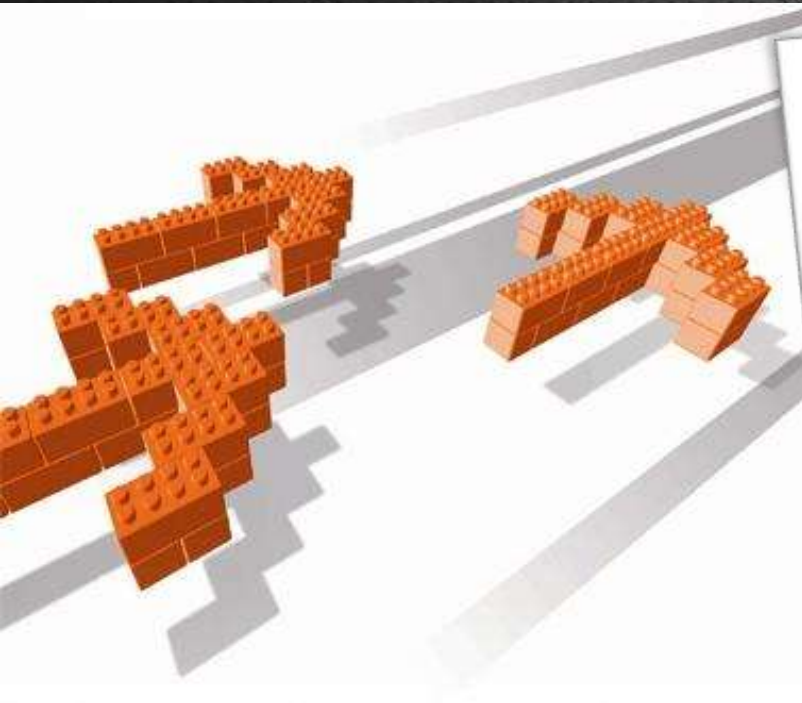


# Q&A

**HELP!**



[lebahnet@cybersecurity.my](mailto:lebahnet@cybersecurity.my)



*Corporate Office:*

**CyberSecurity Malaysia,**

Level 8, Block A,

Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City,

43300 Seri Kembangan,

Selangor Darul Ehsan, Malaysia.

**Tel.** +603 8946 0999

**Fax.** +603 8946 0888

**Hotline.** +1 300 88 2999

**[www.cybersecurity.my](http://www.cybersecurity.my)**

# Thank You