Katsuni理论介绍以及在沙盒和软件仿真方面的应用

Jonathan Brossard (Toucan System)

25/09/2013

我是谁？

- 安全研究人员, 从2005年开始发表一些文章.
- 以往的研究:

  BIOSes漏洞,
  Microsoft Bitlocker,
  Truecrypt,
  McAfee Endpoint (Defcon 2008),
  PMCMA debugger (Blackhat USA 2011),
  « Rakshasa » supply chain backdoor PoC (Blackhat 2012),
  2 SAP notes (2013).
- 在 HITB, CCC, Ruxcon做演讲以及培训...
- Hackito Ergo Sum 以及 NoSuchCon 研究会议的联合创始人 (France).

2013年在防毒软件业中的热点问题?

防毒软件业: 2013年趋势

- 桌面杀毒软件已经是个过去式了

-人们将注意力放在能够检测0day的技术，例如沙盒技术

=> 仿真和沙盒技术是两个比较新兴的事物.

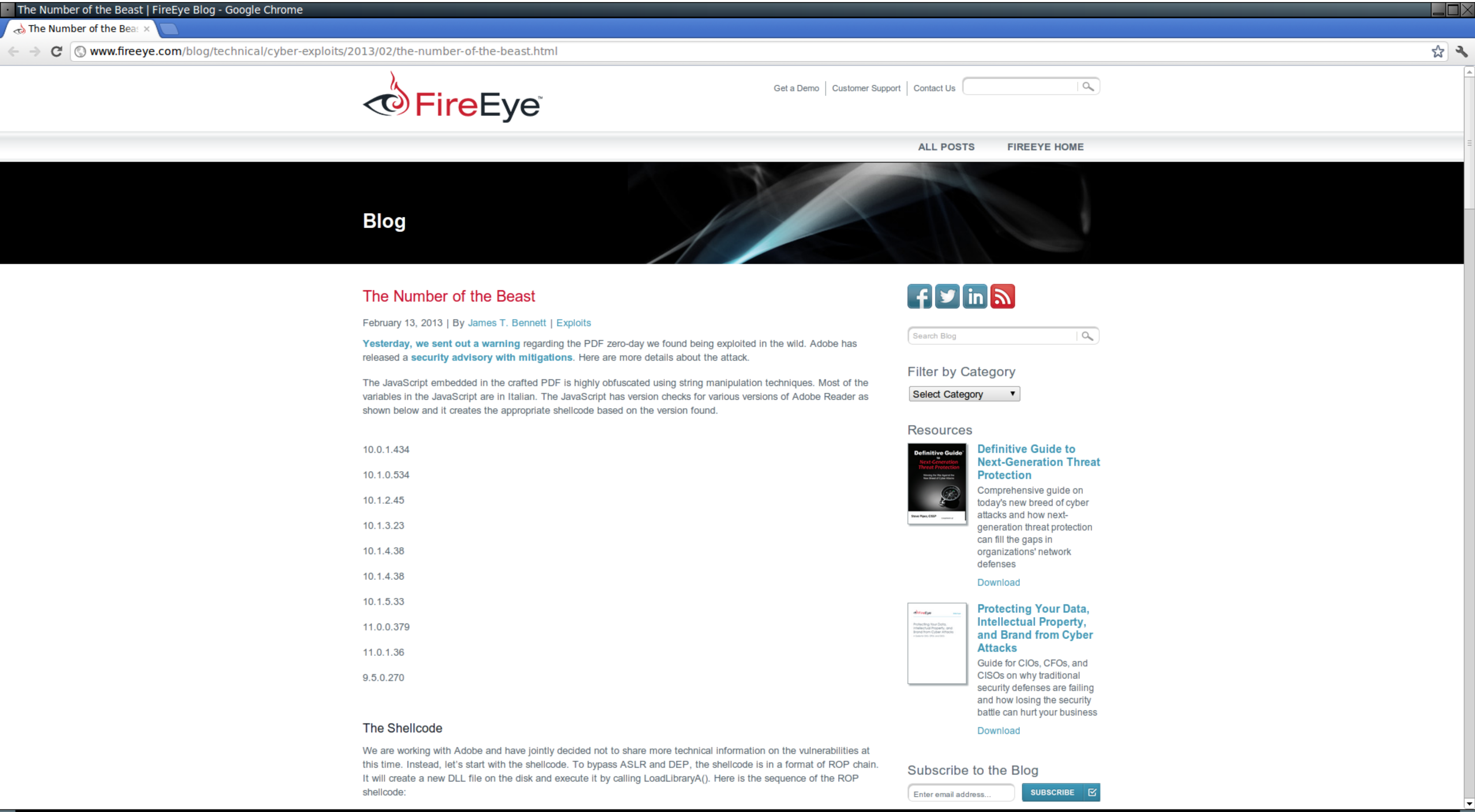
[1] 先别笑.

这些是如何开始的...

CVE-2013-0640
(绕过Adobe 沙盒)

Adobe Reader 以及
Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02
在2013年2月发生的，通过构造恶意PDF文档允许远程攻击者执行任意代码或者引起DOS
(内存崩溃) .

CVE-2013-0640
(绕过Adobe Sandbox)


The Number of the Beast | FireEye Blog - Google Chrome
The Number of the Bea: ×
www.fireeye.com/blog/technical/cyber-exploits/2013/02/the-number-of-the-beast.html
FireEye
Get a Demo | Customer Support | Contact Us
ALL POSTS
FIREEYE HOME
Blog

The Number of the Beast

February 13, 2013 | By James T. Bennett | Exploits

Yesterday, we sent out a warning regarding the PDF zero-day we found being exploited in the wild. Adobe has released a **security advisory with mitigations**. Here are more details about the attack.

The JavaScript embedded in the crafted PDF is highly obfuscated using string manipulation techniques. Most of the variables in the JavaScript are in Italian. The JavaScript has version checks for various versions of Adobe Reader as shown below and it creates the appropriate shellcode based on the version found.

10.0.1.434

10.1.0.534

10.1.2.45

10.1.3.23

10.1.4.38

10.1.4.38

10.1.5.33

11.0.0.379

11.0.1.36

9.5.0.270

The Shellcode

We are working with Adobe and have jointly decided not to share more technical information on the vulnerabilities at this time. Instead, let's start with the shellcode. To bypass ASLR and DEP, the shellcode is in a format of ROP chain. It will create a new DLL file on the disk and execute it by calling LoadLibraryA(). Here is the sequence of the ROP shellcode:

Search Blog
Filter by Category
Select Category ▼
Resources
Definitive Guide to Next-Generation Threat Protection
Comprehensive guide on today's new breed of cyber attacks and how next-generation threat protection can fill the gaps in organizations' network defenses
Download
Protecting Your Data, Intellectual Property, and Brand from Cyber Attacks
Guide for CIOs, CFOs, and CISOs on why traditional security defenses are failing and how losing the security battle can hurt your business
Download
Subscribe to the Blog
Enter email address...
SUBSCRIBE

他们的 « 分析过程 » :

ROP shellcode如下:

msvcr100!fsopen()
msvcr100!write()
mvvcr100!fclose()
kernel32!LoadLibraryA()
kernel32!Sleep()

在加载恶意库文件时,它会进入一个长休眠过程以确保在创建ROP链时所更改的整个栈不会导致线程崩溃。

他们的 « 分析过程 » :

ROP shellcode如下:
msvcr100!fsopen()
msvcr100!write()
mvvcr100!fclose()
kernel32!LoadLibraryA()
kernel32!Sleep()

在加载恶意库文件时, 它会进入一个长休眠过 OP链时所更改的整个栈不会导致线程崩溃。

他们的 « 分析过程 » :

ROP shellcode如下:
msvcr100!fsopen()
msvcr100!write()
mvvcr100!fclose()
kernel32!LoadLibraryA()
kernel32!Sleep()

在加载恶意库文件时, 它会进入一个长休眠过程以确保在创建ROP链时所更改的整个栈不会导致线程崩溃。

=>狗屁不通！他们知道利用代码是在干什么吗？

我猜

小憩5分钟就是为了绕过沙盒检测，哈哈

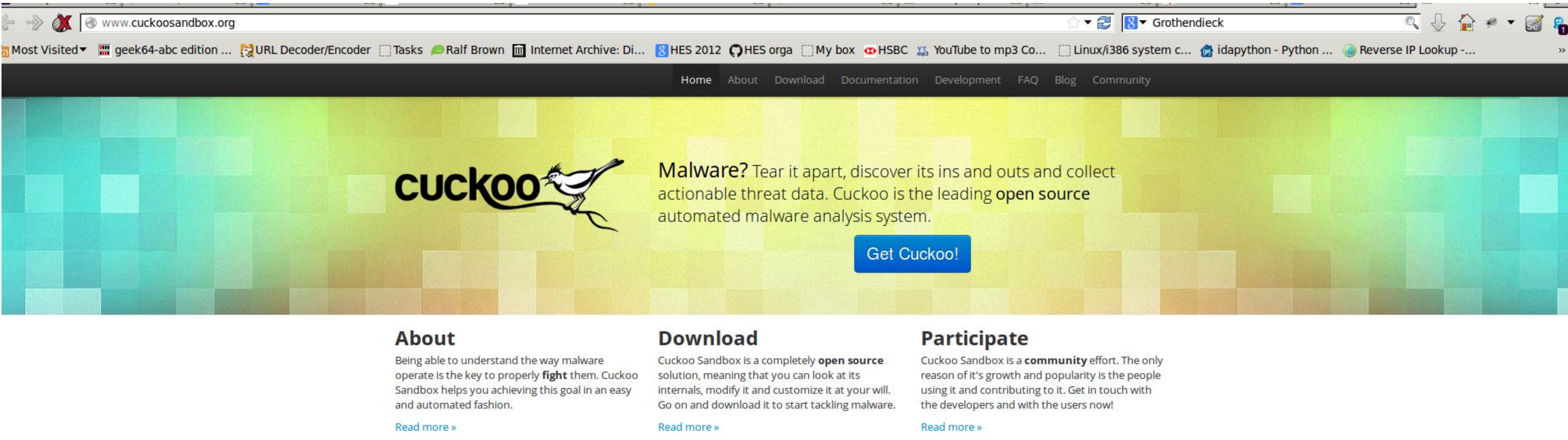
毕竟,它是一个牛叉的利用过程, 第一个去绕过 Adobe的沙盒技术...

这类方法是有缺点的 (恕我直言)

- 擅长于寻找artefacts等玩意儿 (它仍然是« 某些东西 »).
- 但很难理解利用的过程中到底做了什么事情

话虽这么说...

沙盒技术的提高…



Malware? Tear it apart, discover its ins and outs and collect actionable threat data. Cuckoo is the leading **open source** automated malware analysis system.

About

Being able to understand the way malware operate is the key to properly **fight** them. Cuckoo Sandbox helps you achieving this goal in an easy and automated fashion.

Read more »

Download

Cuckoo Sandbox is a completely **open source** solution, meaning that you can look at its internals, modify it and customize it at your will. Go on and download it to start tackling malware.

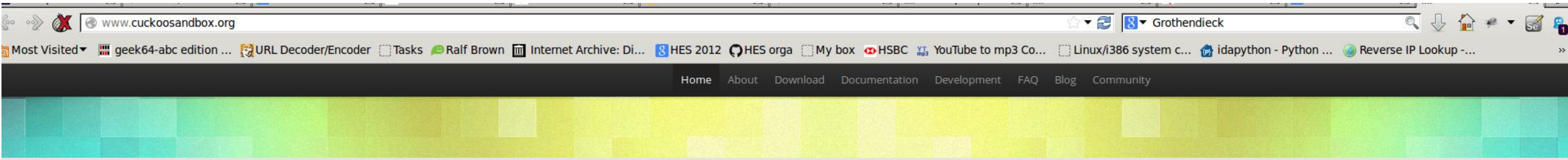
Read more »

Participate

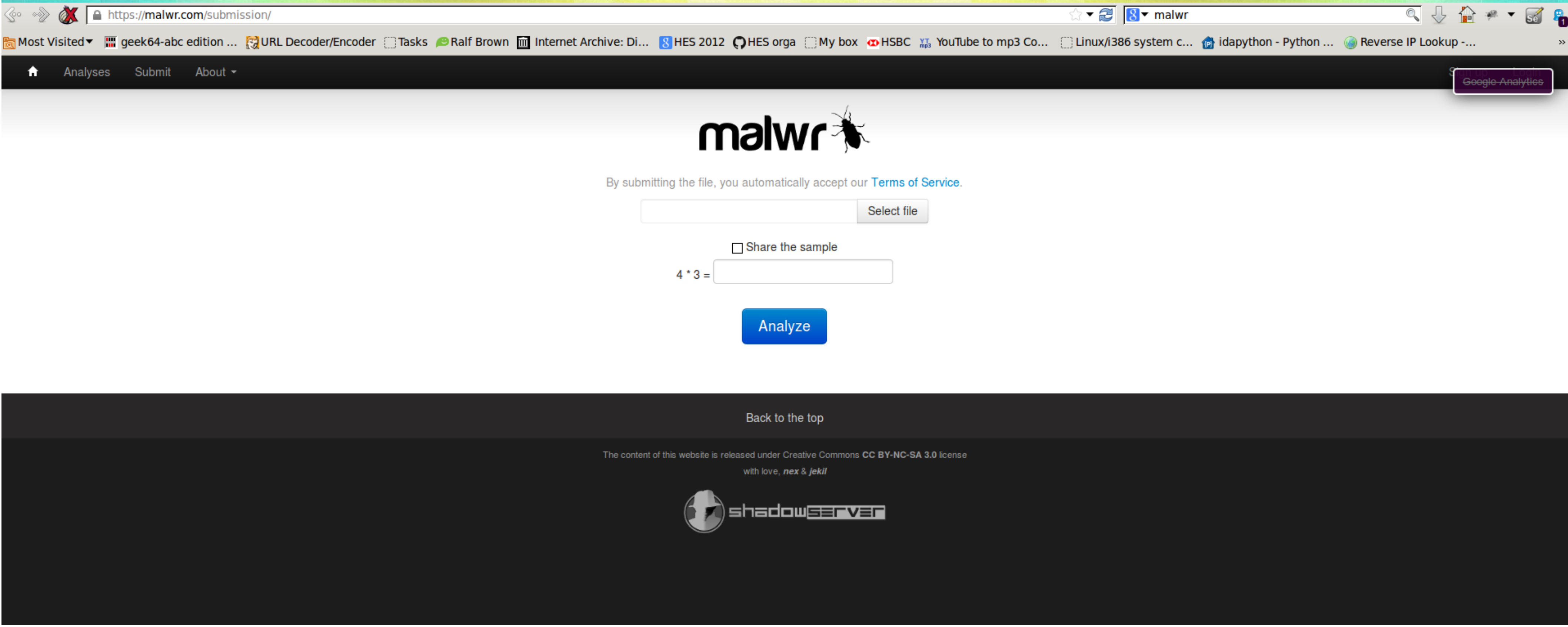
Cuckoo Sandbox is a **community** effort. The only reason of it's growth and popularity is the people using it and contributing to it. Get in touch with the developers and with the users now!

Read more »

沙盒技术的提高…



www.cuckoosandbox.org



https://malwr.com/submission/

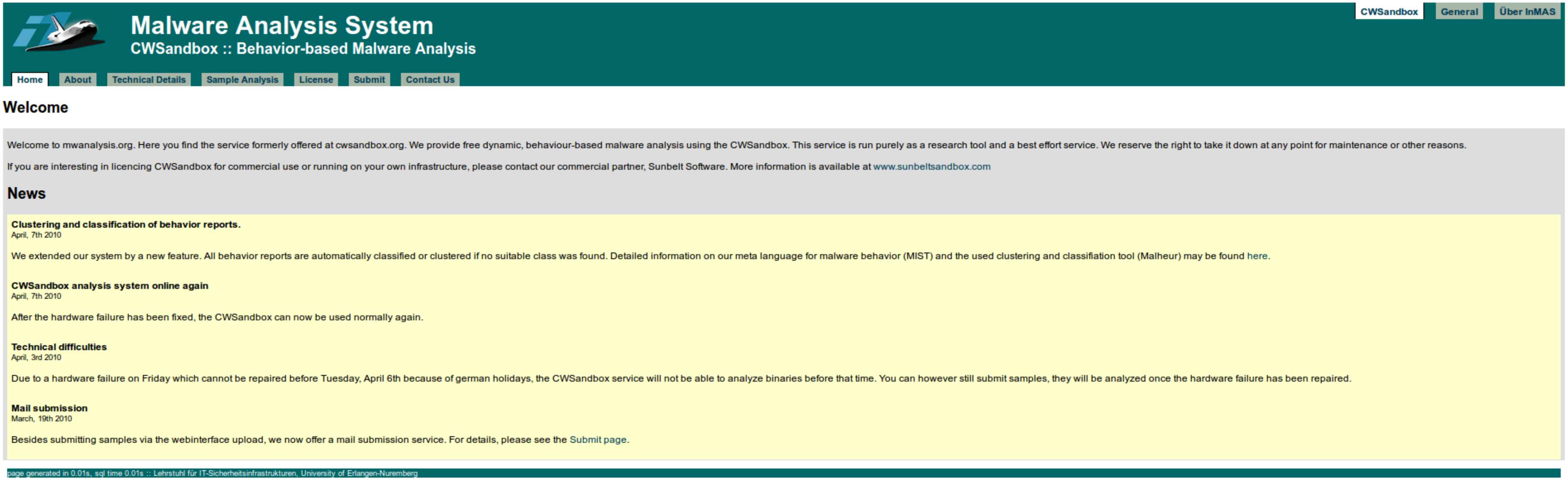
By submitting the file, you automatically accept our Terms of Service.

□ Share the sample

4 * 3 =

with love, ***nex*** & ***jekil***

沙盒技术的提高…



Malware Analysis System

CWSandbox :: Behavior-based Malware Analysis

Welcome

Welcome to mwanalysis.org. Here you find the service formerly offered at cwsandbox.org. We provide free dynamic, behaviour-based malware analysis using the CWSandbox. This service is run purely as a research tool and a best effort service. We reserve the right to take it down at any point for maintenance or other reasons.

If you are interesting in licencing CWSandbox for commercial use or running on your own infrastructure, please contact our commercial partner, Sunbelt Software. More information is available at www.sunbeltsandbox.com

News

Clustering and classification of behavior reports.
April, 7th 2010

We extended our system by a new feature. All behavior reports are automatically classified or clustered if no suitable class was found. Detailed information on our meta language for malware behavior (MIST) and the used clustering and classifiation tool (Malheur) may be found here.

CWSandbox analysis system online again
April, 7th 2010

After the hardware failure has been fixed, the CWSandbox can now be used normally again.

Technical difficulties
April, 3rd 2010

Due to a hardware failure on Friday which cannot be repaired before Tuesday, April 6th because of german holidays, the CWSandbox service will not be able to analyze binaries before that time. You can however still submit samples, they will be analyzed once the hardware failure has been repaired.

Mail submission
March, 19th 2010

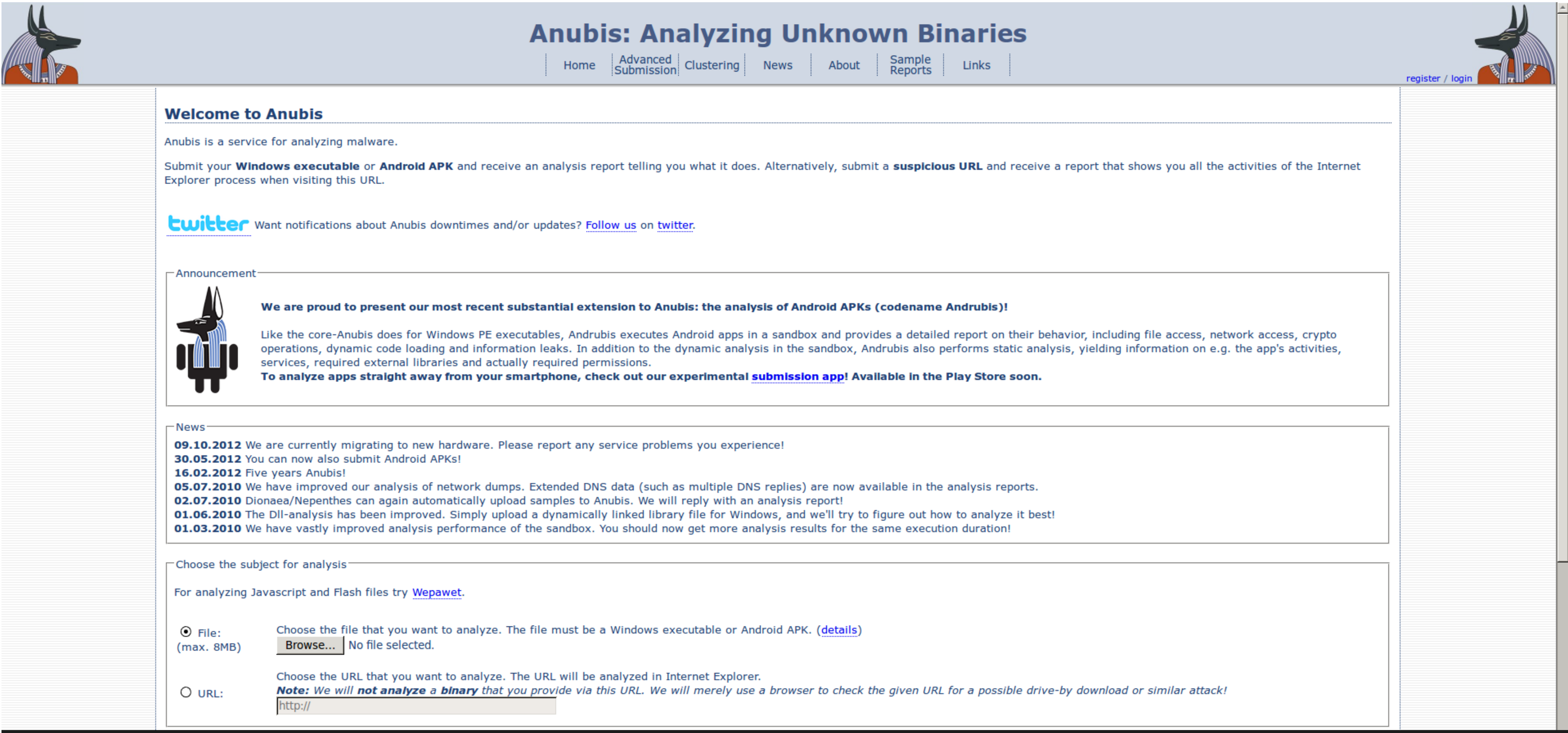
Besides submitting samples via the webinterface upload, we now offer a mail submission service. For details, please see the Submit page.

page generated in 0.01s, sql time 0.01s :: Lehrstuhl für IT-Sicherheitsinfrastrukturen, University of Erlangen-Nuremberg

Back to the top

with love, ***nex*** & ***jekil***

沙盒技术的提高…



Welcome to Anubis

Anubis is a service for analyzing malware.

Submit your **Windows executable** or **Android APK** and receive an analysis report telling you what it does. Alternatively, submit a **suspicious URL** and receive a report that shows you all the activities of the Internet Explorer process when visiting this URL.

twitter Want notifications about Anubis downtimes and/or updates? Follow us on twitter.

Announcement

We are proud to present our most recent substantial extension to Anubis: the analysis of Android APKs (codename Andrubis)!

Like the core-Anubis does for Windows PE executables, Andrubis executes Android apps in a sandbox and provides a detailed report on their behavior, including file access, network access, crypto operations, dynamic code loading and information leaks. In addition to the dynamic analysis in the sandbox, Andrubis also performs static analysis, yielding information on e.g. the app's activities, services, required external libraries and actually required permissions.
To analyze apps straight away from your smartphone, check out our experimental submission app! Available in the Play Store soon.

News

09.10.2012 We are currently migrating to new hardware. Please report any service problems you experience!
30.05.2012 You can now also submit Android APKs!
16.02.2012 Five years Anubis!
05.07.2010 We have improved our analysis of network dumps. Extended DNS data (such as multiple DNS replies) are now available in the analysis reports.
02.07.2010 Dionaea/Nepenthes can again automatically upload samples to Anubis. We will reply with an analysis report!
01.06.2010 The Dll-analysis has been improved. Simply upload a dynamically linked library file for Windows, and we'll try to figure out how to analyze it best!
01.03.2010 We have vastly improved analysis performance of the sandbox. You should now get more analysis results for the same execution duration!

Choose the subject for analysis

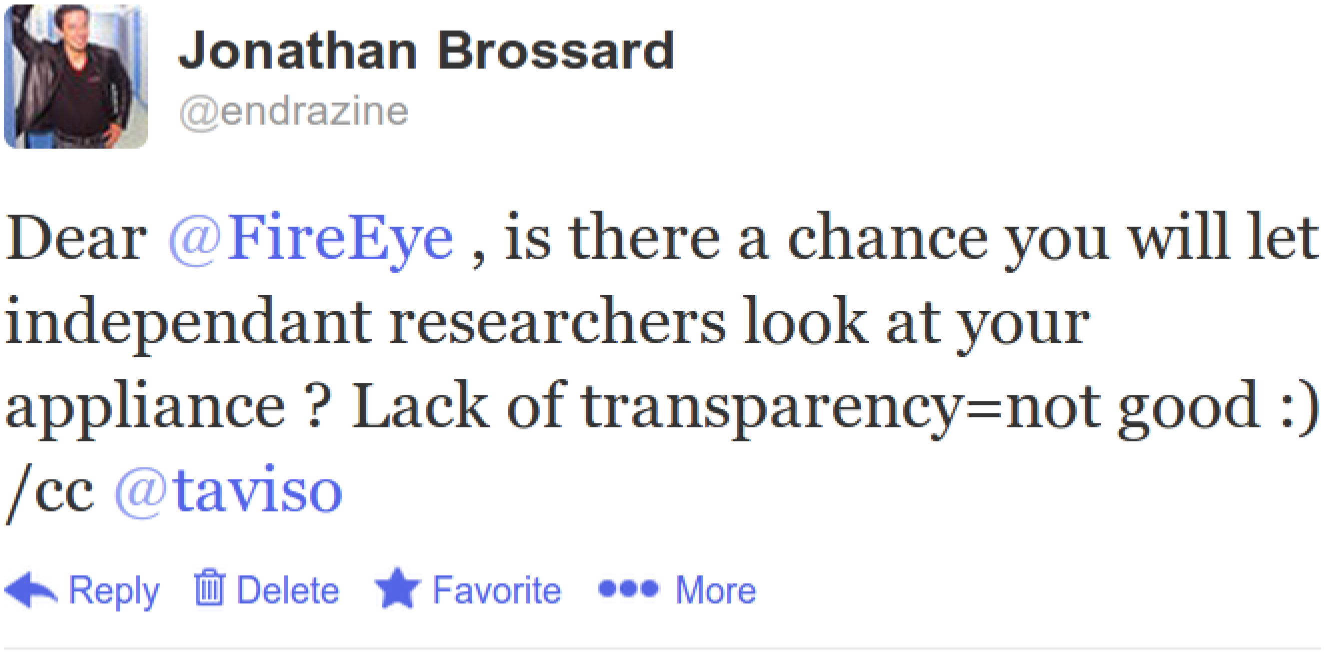
For analyzing Javascript and Flash files try Wepawet.

● File: (max. 8MB) Choose the file that you want to analyze. The file must be a Windows executable or Android APK. (details)
Browse... No file selected.

○ URL: Choose the URL that you want to analyze. The URL will be analyzed in Internet Explorer.
Note: *We will* ***not analyze*** *a* ***binary*** *that you provide via this URL. We will merely use a browser to check the given URL for a possible drive-by download or similar attack!*
http://

我还没有找到一个十分合适的理由去让你在你公司的网络中加入一些没人能够解释的东西进去

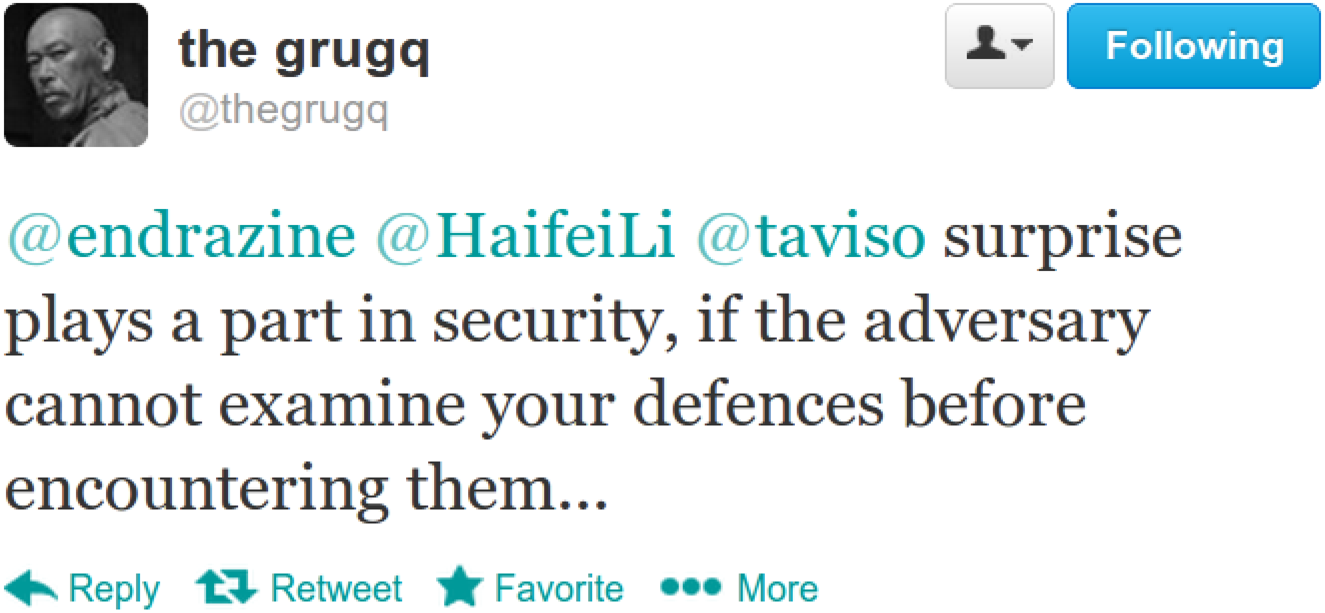
注意: 缺少第三方评估



Jonathan Brossard
@endrazine

Dear @FireEye , is there a chance you will let independant researchers look at your appliance ? Lack of transparency=not good :) /cc @taviso

注意: 缺少第三方评估

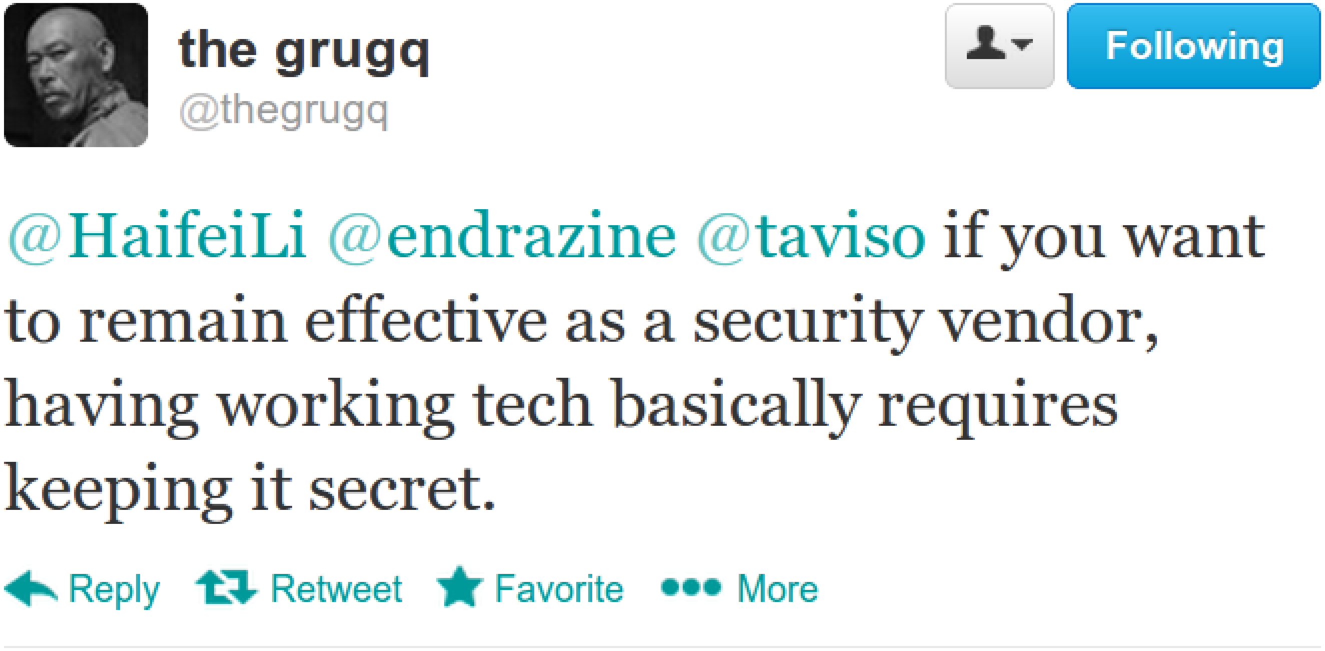


the grugq
@thegrugq

Following

@endrazine @HaifeiLi @taviso surprise plays a part in security, if the adversary cannot examine your defences before encountering them...

注意: 缺少第三方评估



the grugq

@thegrugq

@HaifeiLi @endrazine @taviso if you want to remain effective as a security vendor, having working tech basically requires keeping it secret.

注意: 缺少第三方评估

使用沙盒技术的厂商所提倡的概念就是让假想敌不要看到所使用的技术。好吧，我同意这一点。

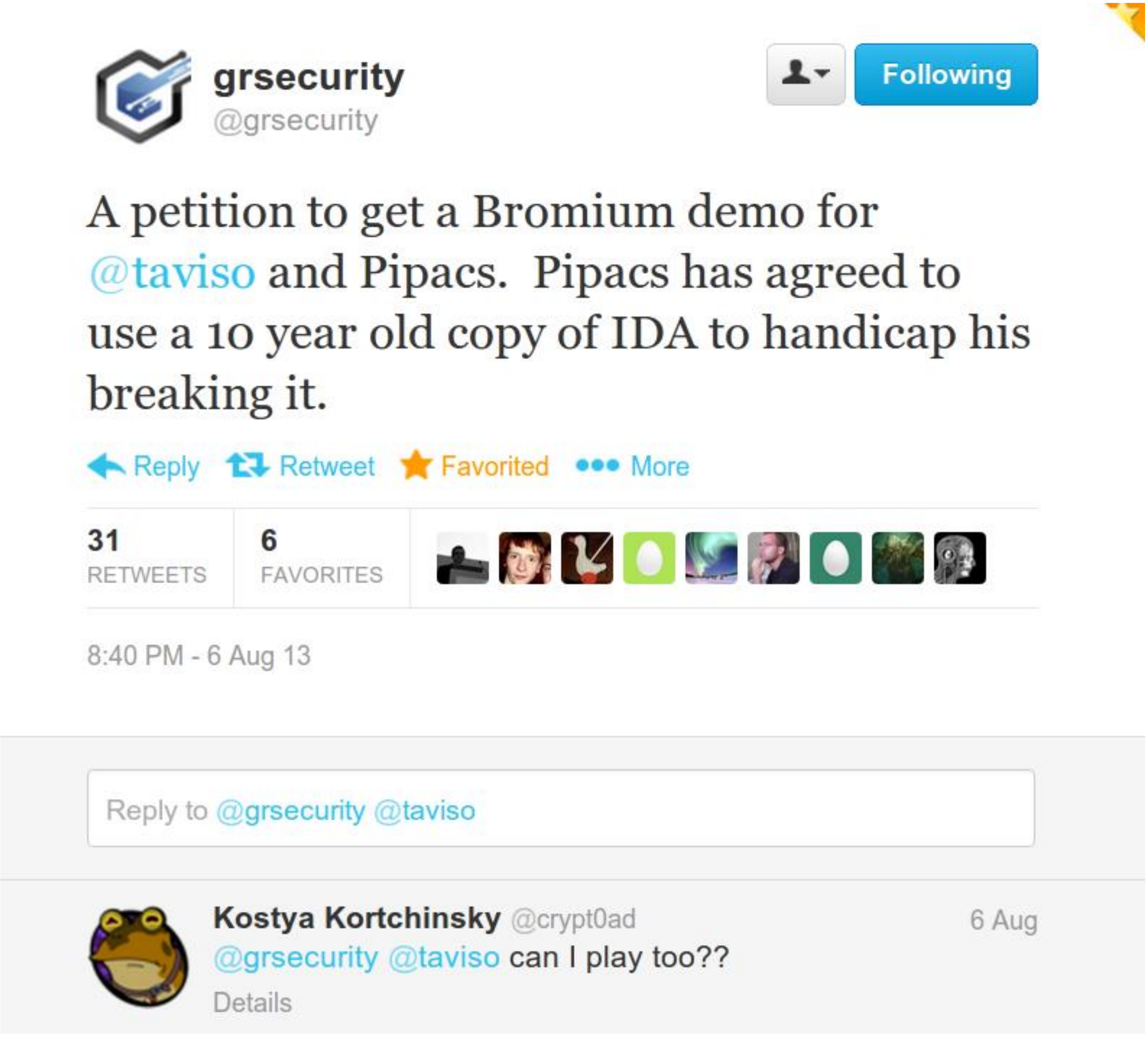
注意: 缺少第三方评估

但是这也意味着做安全的没有（无法？）进行第三方评估

在现实生活中, 通常都是需要这些做安全的进行严格评估的

Tavis Ormandi 和Pipacs也希望看一下Bromium的技术…

注意 : 好吧, 他们不是Bromium的客户, 因此我们有了麻烦... 作为一个行业, 确实如此.



grsecurity @grsecurity

A petition to get a Bromium demo for @taviso and Pipacs. Pipacs has agreed to use a 10 year old copy of IDA to handicap his breaking it.

31 RETWEETS 6 FAVORITES

8:40 PM - 6 Aug 13

Kostya Kortchinsky @crypt0ad 6 Aug

@grsecurity @taviso can I play too??

问题所在
(研究导向)

毕竟...

目前 « 好一些的 » 思路:

- 关联/分享更多的数据以创建信息不对称.
- 为此, 目前绝大部分 (我所看到的允许他, 至少在非默认模式下) 解决方案允许恶意代码连向Internet [*].

[*] 例如在敌人攻击时，希望通过将DNS/二进制校验信息进行关联的想法

真实的情况...

- 在过去15年，整个公司的策略就是确保LANS, DMZs 以及internet的隔离.
- 如今你在网络边界（代理、邮件网关、任何能够让沙盒存在的地方）给攻击者一个临时shell ...

- … 同时在你DNS上发生了什么？

Katsuni-Kaminsky 攻击
(两全其美的方案)

- 攻击者可以在一个沙盒内运行恶意代码.
- 沙盒允许攻击者反向连接Internet.
- 公司的DNS服务器被用作递归DNS服务器.
- 攻击者可以衡量两个方面同时能够将来自网络内部和外部的喷射数据包进行同步.

=> 很明显这样做是很 « 安全的 »...

更不用提...

- 如果在沙盒中的恶意代码想办法攻击其他网络 other networks (say crowdstrike !) ?
- 如果恶意代码向自己的网络中发送一个修改的版本 (smtp?) 为了更多的分析以及更多的沙盒CPU时间?

=> 所有这些都只是实现的问题.

将bugs放到沙盒中去

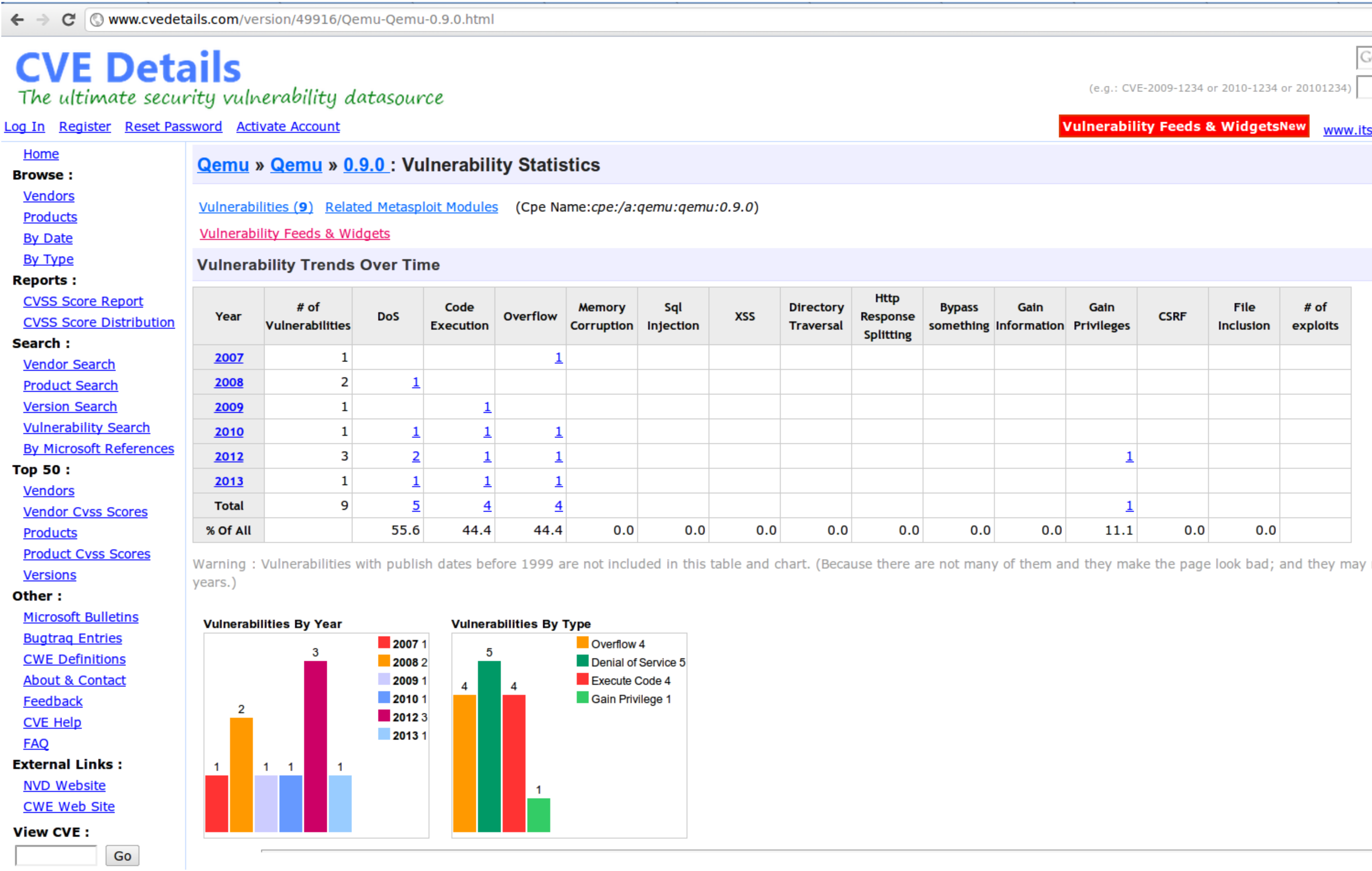
问题所在

- 很多在线恶意代码的扫描引擎运行qemu (以及一些各类设备和自动化定制软件)
- 用户根本看不到这些扫描的进程在干什么.
- 这样的话，如果攻击者发起一个基于qemu的DoS会怎么样？

将bugs放到沙盒中去

(又名：hacking 在线恶意代码分析工具…)

这样的bug确实存在...



www.cvedetails.com/version/49916/Qemu-Qemu-0.9.0.html

CVE Details

The ultimate security vulnerability datasource

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register Reset Password Activate Account

Vulnerability Feeds & WidgetsNew www.its

Home

Browse :

- Vendors
- Products
- By Date
- By Type

Reports :

- CVSS Score Report
- CVSS Score Distribution

Search :

- Vendor Search
- Product Search
- Version Search
- Vulnerability Search
- By Microsoft References

Top 50 :

- Vendors
- Vendor Cvss Scores
- Products
- Product Cvss Scores
- Versions

Other :

- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ

External Links :

- NVD Website
- CWE Web Site

View CVE :

Go

Qemu » Qemu » 0.9.0 : Vulnerability Statistics

Vulnerabilities (9) Related Metasploit Modules (Cpe Name:*cpe:/a:qemu:qemu:0.9.0*)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
2007	1			1											
2008	2	1													
2009	1		1												
2010	1	1	1	1											
2012	3	2	1	1								1			
2013	1	1	1	1											
Total	9	5	4	4								1			
% Of All		55.6	44.4	44.4	0.0	0.0	0.0	0.0	0.0	0.0	0.0	11.1	0.0	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may years.)

Vulnerabilities By Year

Vulnerabilities By Type

Qemu 内部机理

Qemu 目标

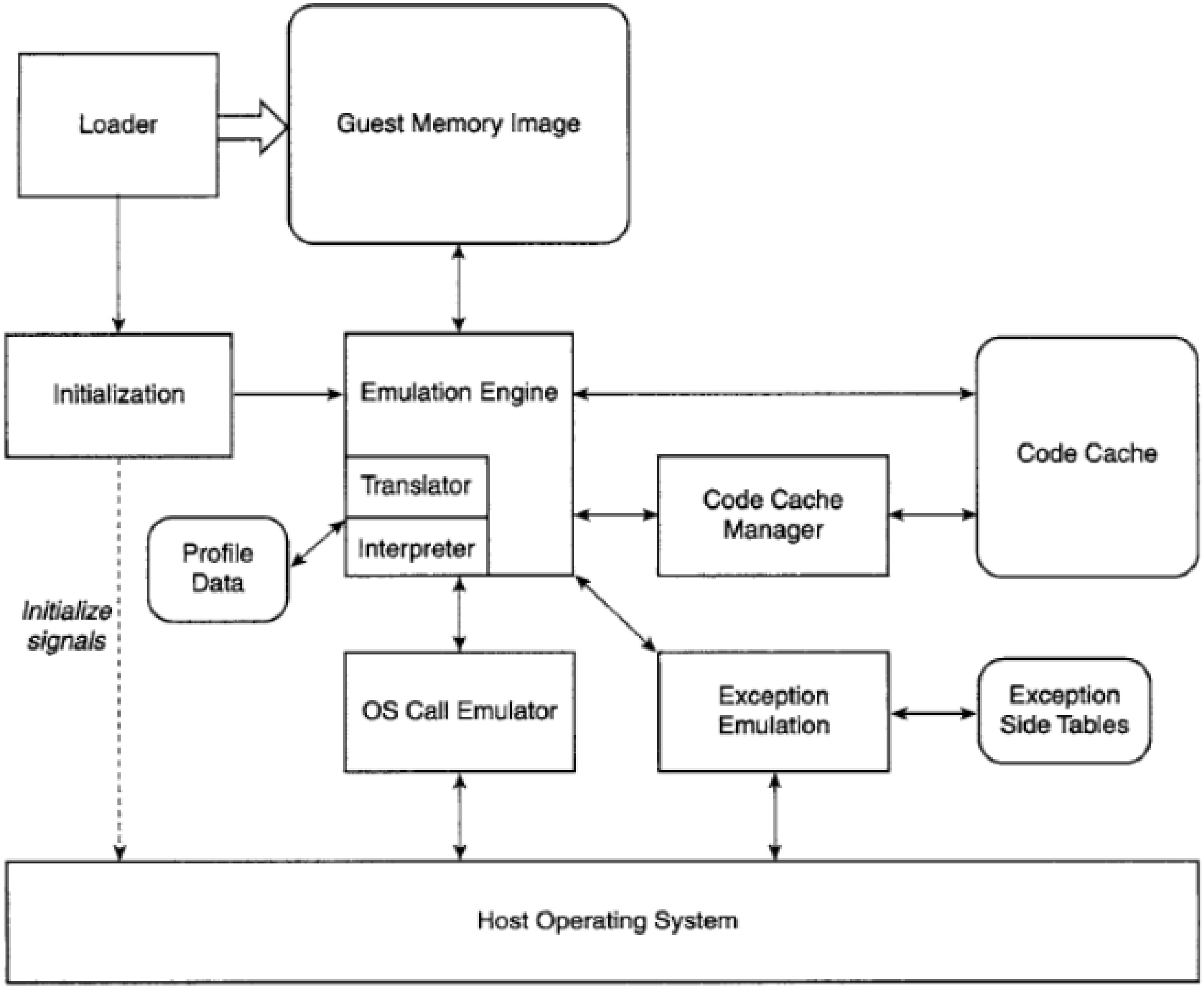
- (快速) 二进制翻译
- 二进制代码被翻译成被虚拟CPU执行的IR, 独立于主机.
- 很通用，很快速，很好的可移植性，很酷！不可思议的工具！
- 不过在分析恶意代码时是否很安全，有待考究？

Qemu 支持两个模式

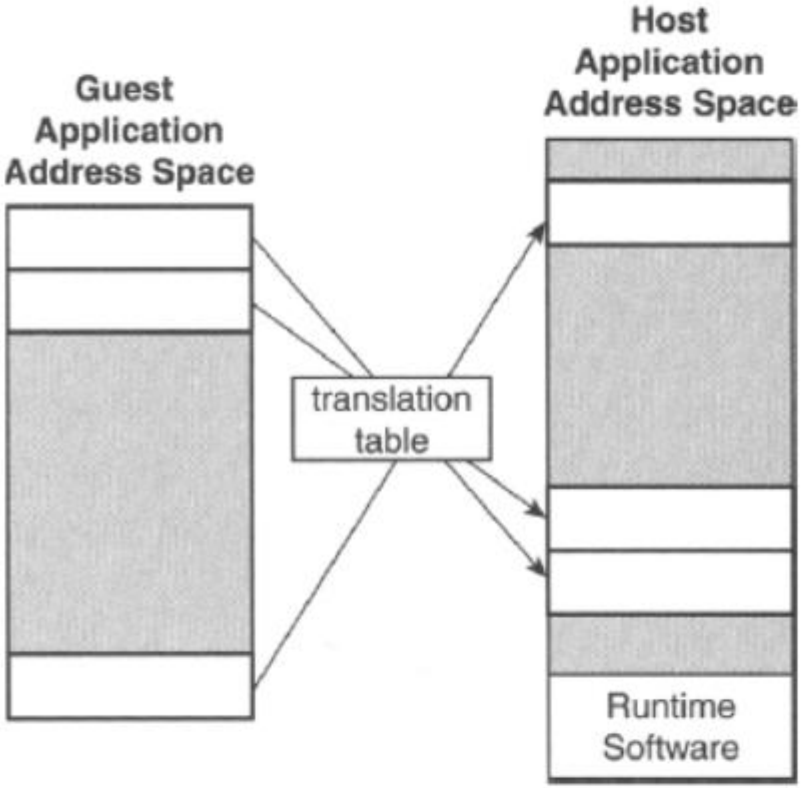
- 系统(全部)虚拟化
- 内核仿真 (wine/Windows, linux).

虽然目前大多数实现都使用第一种方式，
但我们将关注第二种,因为它能保证更快的速度增强以及更好的攻击面 ;)

Qemu 框架

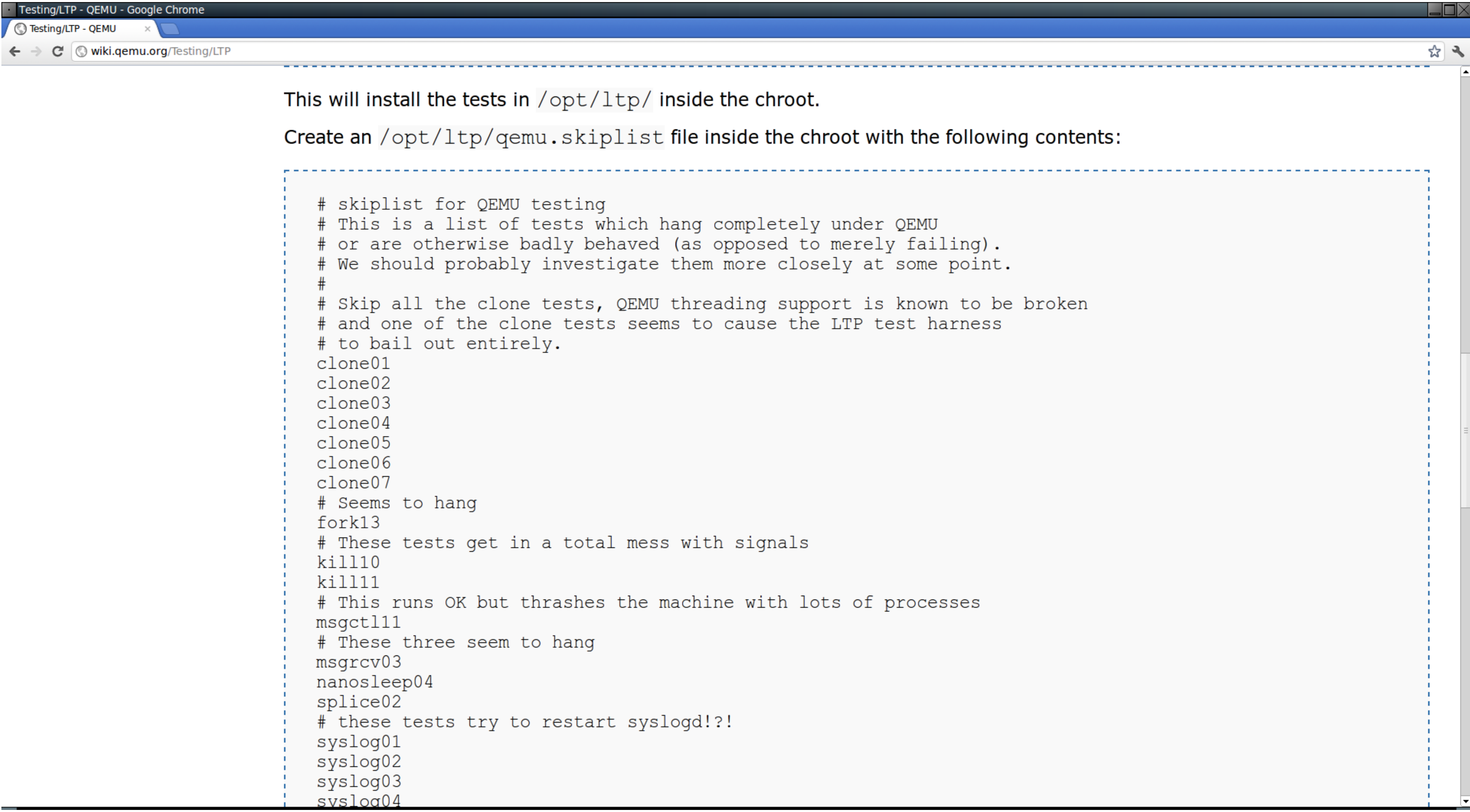

Loader
Guest Memory Image
Initialization
Emulation Engine
Translator
Interpreter
Code Cache
Code Cache Manager
Profile Data
Initialize signals
OS Call Emulator
Exception Emulation
Exception Side Tables
Host Operating System

理解二进制翻译和内存共享


Guest Application Address Space
translation table
Host Application Address Space
Runtime Software

派对时间 !!

Qemu 回归测试...



This will install the tests in `/opt/ltp/` inside the chroot.

Create an `/opt/ltp/qemu.skiplist` file inside the chroot with the following contents:

```
# skiplist for QEMU testing
# This is a list of tests which hang completely under QEMU
# or are otherwise badly behaved (as opposed to merely failing).
# We should probably investigate them more closely at some point.
#
# Skip all the clone tests, QEMU threading support is known to be broken
# and one of the clone tests seems to cause the LTP test harness
# to bail out entirely.
clone01
clone02
clone03
clone04
clone05
clone06
clone07
# Seems to hang
fork13
# These tests get in a total mess with signals
kill10
kill11
# This runs OK but thrashes the machine with lots of processes
msgctl11
# These three seem to hang
msgrcv03
nanosleep04
splice02
# these tests try to restart syslogd!?!
syslog01
syslog02
syslog03
syslog04
```

Demos

总结

有趣的技术. 很酷的hacking工具.

这里仍然有很多问题存在于细节当中.

就我所知，尚未有第三方评估.

从博弈论上来看, 一个人最大的收益就是让别人使用某项技术，但自己却远离不要用它…

Katsuni-Grothendieck理论能够很好的应对沙盒技术中的0day问题:

« 这里没有两全其美的方案！»

很荣幸能够参会.

问题？