

PHÁT HIỆN MÃ ĐỘC

TỰ ĐỘNG

NGÔ VĂN NHẬN
NGUYỄN VĂN GIỎI
ĐỖ BÁ NGUYỄN

PHÂN TÍCH MÃ ĐỘC

LÀ GÌ?

Phát hiện hành vi, cấu trúc của các loại mã độc, từ đó tìm ra cách thức lây lan, phát tán, nguồn phát tán, mức độ nguy hiểm... của mã độc; cách phòng chống, khắc phục hậu quả do mã độc đó gây ra



Malware



Static Analysis



Dynamic Analysis



Memory Analysis

QUY TRÌNH
PHÂN TÍCH

Reports



PHÂN TÍCH TĨNH

DỊCH NGƯỢC

Đòi hỏi người phân tích xem xét kỹ mã của virus, hiểu được luồng thực thi và các hành vi của nó thông qua mã đã dịch ngược



Bê



PHÂN TÍCH ĐỘNG

CHẠY THỰC TẾ

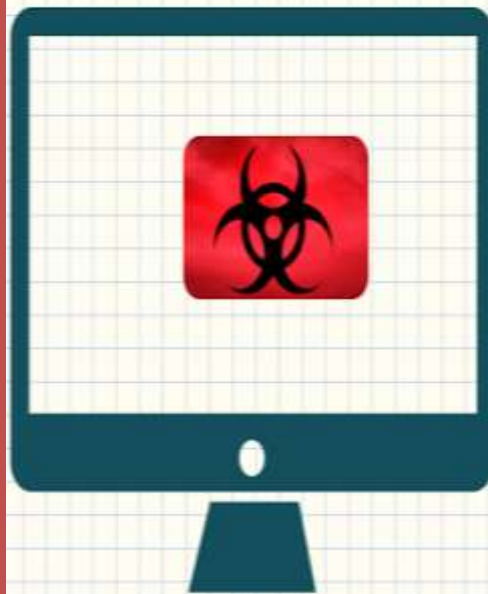
Phân tích cách hoạt động của virus khi nó được thực thi, nó đã kết nối đến đâu, lây lan như thế nào, cài đặt những gì vào hệ thống, thay đổi thành phần nào, hoạt động ra sao



Bê



Analysis Machine



ip: 192.168.1.150

gw: 192.168.1.3

dns: 4.2.2.2

PHÂN TÍCH MÃ ĐỘC TỰ ĐỘNG

HỆ THỐNG PHÁT HIỆN MÃ ĐỘC

 **Malheur**
Automatic Analysis

VIRUSTOTAL

[HTTP://VIRUSTOTAL.COM](http://VIRUSTOTAL.COM)

- ✓ Phân tích tự động
- ✓ Có sự tham gia của rất nhiều hãng diệt virus uy tín
- ✓ Lấy được các thông tin cơ bản



SANDBOX

LÀ GÌ?

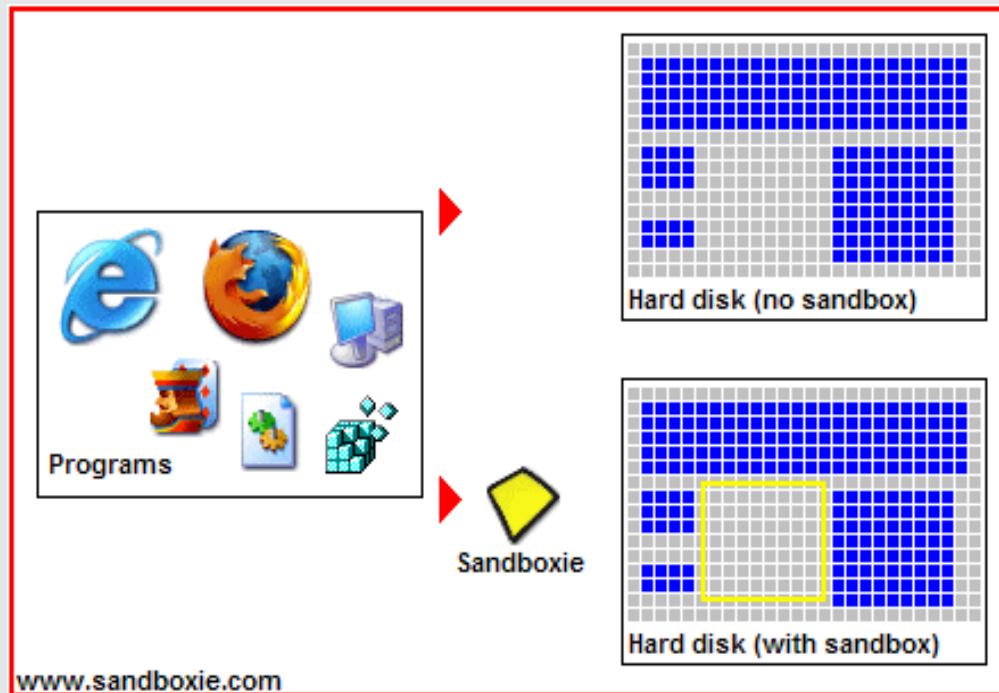
Sandbox là một kỹ thuật rất quan trọng trong bảo mật giúp hạn chế việc truy cập vào tài nguyên hệ thống của các ứng dụng ngoài.

- Một môi trường dùng để chạy phần mềm và môi trường đó được nằm trong sự kiểm soát chặt chẽ.
- Cô lập các ứng dụng, ngăn chặn các phần mềm độc hại để chúng không thể làm hỏng hệ thống máy tính, hay cài cắm các mã độc nhằm ăn cắp thông tin cá nhân
- Sandbox giúp hạn chế chức năng của một đoạn mã, cấp quyền cho một đoạn mã nào đó chỉ được thực hiện một số chức năng nhất định, từ đó nó không thể thực hiện những can thiệp khác có thể làm nguy hại cho máy tính người dùng

SANDBOX

LÀ GÌ?

Sandbox là một kỹ thuật rất quan trọng trong bảo mật giúp hạn chế việc truy cập vào tài nguyên hệ thống của các ứng dụng ngoài.



SANDBOX

DÙNG Ở ĐÂU?

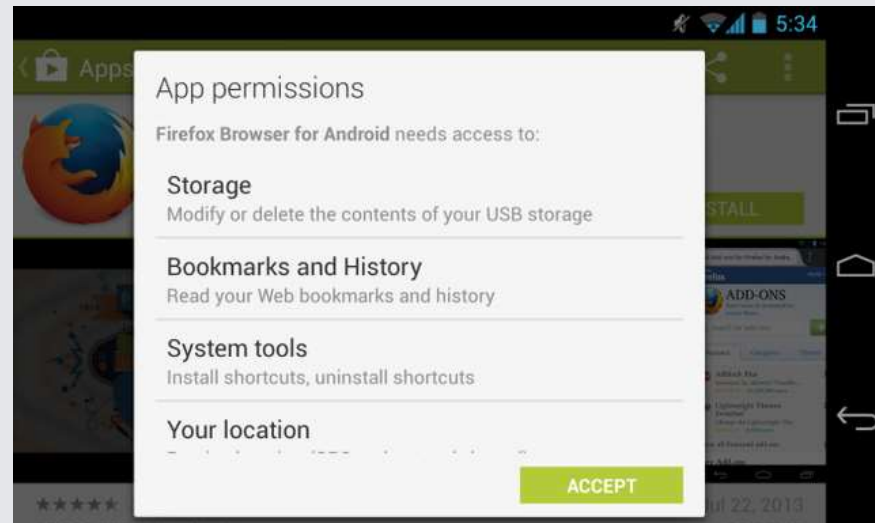
Ứng dụng nào sử dụng Sandbox?

- Các trình duyệt: Cô lập trang web mà nó tải. Khi website cố gắng truy cập vào dữ liệu trên máy, yêu cầu truy cập này sẽ được thông báo tới người sử dụng.
- Plugins trình duyệt: Flash hoặc Silverlight
- Trình đọc PDF, Microsoft Office: Sử dụng Sandbox để ngăn các truy cập không hợp lệ, các macro không an toàn làm hại đến máy tính
- Các hệ điều hành di động: Ngăn các ứng dụng truy cập tài nguyên hệ thống trừ khi người dùng cho phép
- Hệ điều hành: Chức năng User Account Control
- Máy ảo: Cô lập hệ thống ảo với máy thật, đảm bảo không cho các truy cập lạ từ máy ảo ra máy thật

SANDBOX

DÙNG Ở ĐÂU?

Ứng dụng nào sử dụng Sandbox?



CUCKOO SANDBOX

[HTTPS://CUCKOOSANDBOX.ORG/](https://cuckoosandbox.org/)



CUCKOO SANDBOX

LÀ GÌ & LÀM GÌ?

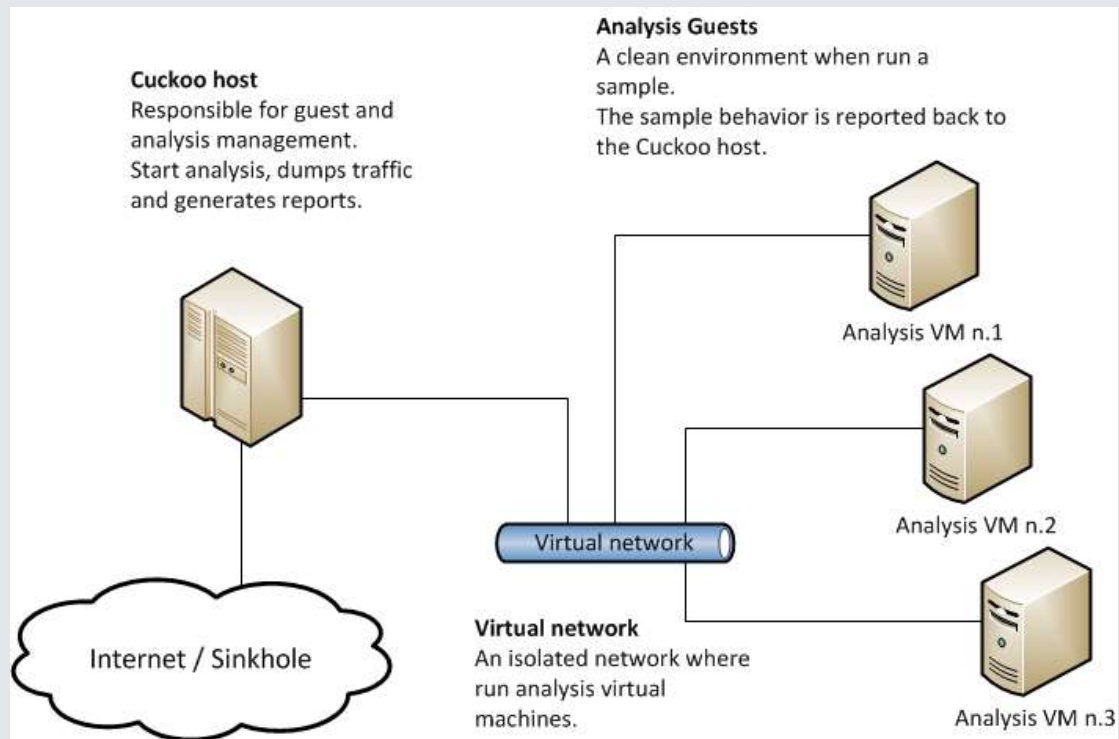
Lịch sử, nguồn gốc, cách thức hoạt động, cấu trúc hệ thống, khả năng hoạt động, giao diện

- Cuckoo Sandbox là dự án được khởi động sau sự kiện Google Summer of Code năm 2010
- Hệ thống phân tích malware động tự động, giám sát những file nghi ngờ trong một môi trường tách biệt
- Tự động thực thi và giám sát hành vi của bất kỳ malware nào qua một máy ảo Windows
- Dữ liệu mà Cuckoo theo dõi được gồm dấu vết API Windows, các lệnh copy, tạo và xóa file, làm tràn bộ nhớ (memory dump) và phân tích cấu hình hệ thống...

CUCKOO SANDBOX

LÀ GÌ & LÀM GÌ?

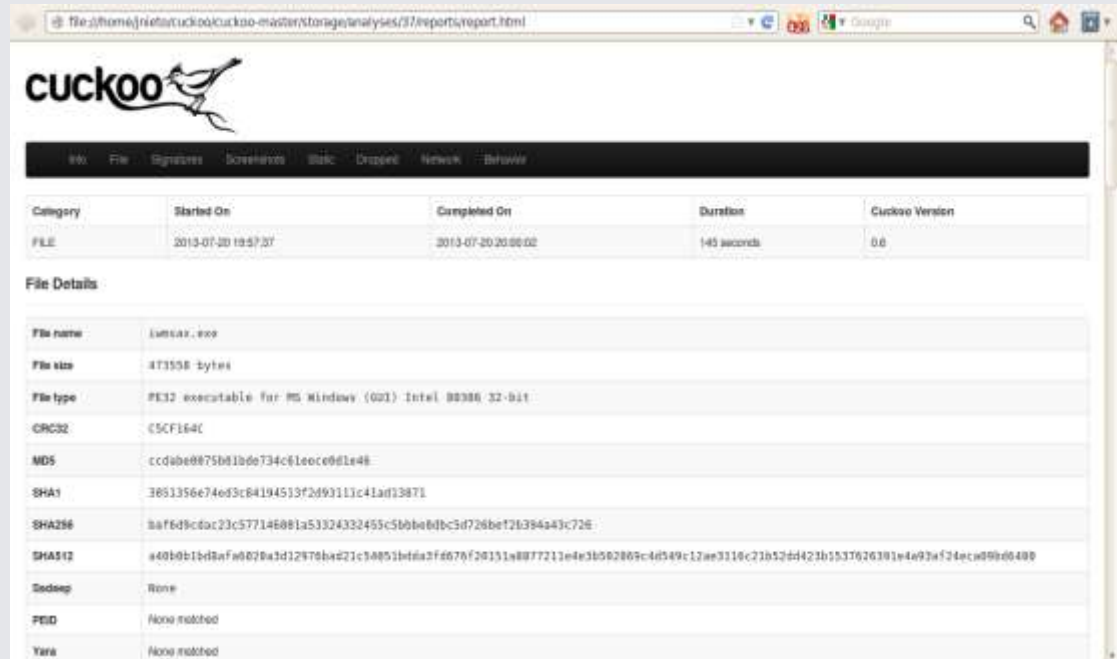
Lịch sử, nguồn gốc, cách thức hoạt động, cấu trúc hệ thống, khả năng hoạt động, giao diện



CUCKOO SANDBOX

LÀ GÌ & LÀM GÌ?

Lịch sử, nguồn gốc, cách thức hoạt động, cấu trúc hệ thống, khả năng hoạt động, giao diện



The screenshot displays the Cuckoo Sandbox web interface in a browser window. The address bar shows the URL: `file:///home/niet/cuckoo/cuckoo-master/storage/analyses/37/reports/report.html`. The page features the Cuckoo logo and a navigation menu with tabs: Info, File, Signatures, Downloads, Static, Dropped, Network, and Behavior. Below the menu is a summary table for the analysis.

Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2013-07-20 19:57:37	2013-07-20 20:00:02	145 seconds	0.0

Below the summary table is the 'File Details' section, which lists various file attributes:

File name	lsmux.exe
File size	473558 bytes
File type	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
CRC32	C5CF164C
MD5	ccda8e875b1bde734c61eece8d1e48
SHA1	3851356e74ed3c84194513f2d93111c41ad13871
SHA256	bafe9dc0ac23c577146881a53324332455c5bbbe6bc3d726bet26384a43c726
SHA512	a40b0b1b18af0878a3d12870ba421c3a851bda2f4676f20151a8877211e4e3b502809c4d549c12ae3116c21b52d4421b5537626301e4a93af24ecw898d0480
Sedseq	None
PEID	None matched
Yara	None matched

THAT'S ALL

THANKS

FOR YOUR TIME

SHORT FOR "TROUBLE"

#BOLDL