
SHALL WE PLAY A GAME?

da Jessica a Mr. Robot

quando l'immaginario hacker incontra la realtà

Matteo 'fusys' Falsetti

Giantranco 'DDK' Ciotti

un pollo in ogni forno e uno smartphone in ogni tasca

Lecco, 28/01/2020

The Italian Job, 1969

Troy Kennedy-Martin

The Italian Job, 2003

Troy Kennedy-Martin, Donna Powers


MICHAEL CAINE NOËL COWARD
THE ITALIAN JOB


2SBI658


THE
ITALIAN
JOB

realismo praticabilita' Hollywood

Has New York's traffic light system been HACKED? Researcher claims to be able to control Manhattan traffic (and says the same technique will wo

- Re
- Sa
- Us

By M
PUBL

A se
majo

Cesa
traff

He d
usec

Scro

L.A. NOW

SOUTHERN CALIFORNIA -- THIS JUST IN

« Previous Post | L.A. NOW Home | Next Post »

Engineers who hacked into L.A. traffic signal computer, jamming streets, sentenced

DECEMBER 1, 2009 | 7:17 AM

Two L.A. traffic engineers who pleaded guilty to hacking into the city's signal system and slowing traffic at key intersections as part of a labor protest have been sentenced to two years' probation.

Authorities said that Gabriel Murillo, 40, and Kartik Patel, 37, hacked into the system in 2006 despite the city's efforts to block access during a labor action.

Fearful that the strikers could wreak havoc, the city temporarily blocked all engineers from access to the computer that controls traffic signals.

But authorities said Patel and Murillo found a way in and picked their targets with care -- intersections they knew would cause significant backups because they were close to freeways and major destinations.

The engineers programmed the signals so that red lights for several days starting Aug. 21, 2006 would be extremely long on the most congested approaches to the intersections, causing gridlock. Cars backed up at Los Angeles International Airport, at a key intersection in Studio City, at access onto the clogged Glendale Freeway and throughout the streets of Little Tokyo and the L.A. Civic Center area, sources told The Times at the time. No accidents occurred as a result.

As part of their plea deal, the engineers agreed to pay $6,250 in restitution and completed 240 hours of community service.

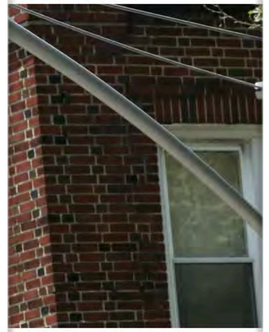
-- Shelby Grad

JALOPNIK Drive Free or Die.

MORNING SHIFT NICE PRICE OR CRACK P

sy To Hack A Tr

41.6K



om the *Italian Job* remake where the
raffic control center and changes all
Turns out that it's not too difficult t

"Green Lights Forever: Analyzing th
ed in 2014 by the Electrical Engineer
he University of Michigan, researche
ity holes in the road agency's traffic
s have been getting new attention t

accessibility of the network to hack
n the network lacking secure authen
mes and passwords, and that the tr
loits.

road agency in Michigan, the resea
at each intersection and were able t
deo camera via an Ethernet connecti

igated uses commercially available
ther 5.8 GHz or 900 Mhz. Figure 3 s

The Washington Post
Democracy Dies in Darkness

Local

Can hackers take over traffic lights?

cer of security

ions. He
, downtown
med with
rough a

revealed
ment of
sensors after

Green Lights Forever: Analyzing the Security of Traffic Infrastructure

Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman
Electrical Engineering and Computer Science Department
University of Michigan
{brghena, wbeyer, hillaker, jpevarne, jhalderm}@umich.edu

Abstract

The safety critical nature of traffic infrastructure requires that it be secure against computer-based attacks, but this is not always the case. We investigate a networked traffic signal system currently deployed in the United States and discover a number of security flaws that exist due to systemic failures by the designers. We leverage these flaws to create attacks which gain control of the system, and we successfully demonstrate them on the deployment in coordination with authorities. Our attacks show that an adversary can control traffic infrastructure to cause disruption, degrade safety, or gain an unfair advantage. We make recommendations on how to improve existing systems and discuss the lessons learned for embedded systems security in general.

1 Introduction

Traffic signals were originally designed as standalone hardware, each running on fixed timing schedules, but have evolved into more complex, networked systems. Traffic controllers now store multiple timing plans, integrate varied sensor data, and even communicate with other intersections in order to better coordinate traffic.

Studies have shown the benefits of a well coordinated traffic signal system in terms of wasted time, environmental impact, and public safety [2], but coordination has been difficult to achieve due to the geographic distribution of roadways and the cost of physical connections between intersections. Wireless networking has helped to mitigate these costs, and many areas now use intelligent wireless traffic management systems [10, 32, 33]. This allows for new capabilities including real-time monitoring and coordination between adjacent intersections. However, these improvements have come with an unintended side effect. Hardware systems that had previously been only physically accessible are now remotely accessible and software controlled, opening a new door for attackers.

To test the feasibility of remote attacks against these systems, we perform a security evaluation of a wireless traffic signal system deployed in the United States. We discover several vulnerabilities in both the wireless network and the traffic light controller. With coordination from the road agency, we successfully demonstrate several attacks against the deployment and are able to change the state of traffic lights on command.

The vulnerabilities we discover in the infrastructure are not a fault of any one device or design choice, but rather show a systemic lack of security consciousness. We use the lessons learned from this system to provide recommendations for both transportation departments and designers of future embedded systems.

2 Anatomy of a Traffic Intersection

The modern traffic intersection is an amalgamation of various sensors, controllers, and networking devices. Figure 1 shows some common devices found at intersections.

2.1 Sensors

Sensors are used to detect cars and inspect infrastructure. Induction loops (also known as in-ground loops) are frequently used to detect vehicles. These devices are buried in the roadway and detect cars by measuring a change in inductance due to the metal body of the vehicle. Video detection is also frequently used to sense vehicles at intersections. In the United States, 79% of all vehicle detection systems use video detection or induction loops [18]. Microwave, radar, and ultrasonic sensors are less common, but also used [17]. Video cameras are also commonly installed to allow remote inspection of the intersection.

2.2 Controllers

Traffic controllers read sensor inputs and control light states. The controller is typically placed in a metal cabinet by the roadside along with relays to activate the traffic lights. Sensors are typically directly connected to the controller, allowing it to combine vehicle detection information with pre-programmed timing controls in order to determine the current state of the traffic lights.

Intersections can be configured to operate in several different modes. In the simplest case, pre-timed mode, lights are controlled solely on preset timings [8]. More complicated controllers function in a semi-actuated mode where the side street is activated based on sensors and the main street otherwise runs continuously. In fully-actuated mode, both streets are serviced based on sensor input [36].

Controllers can function as isolated nodes or as part of an interconnected system. Isolated intersections maintain

Wargames, 1983

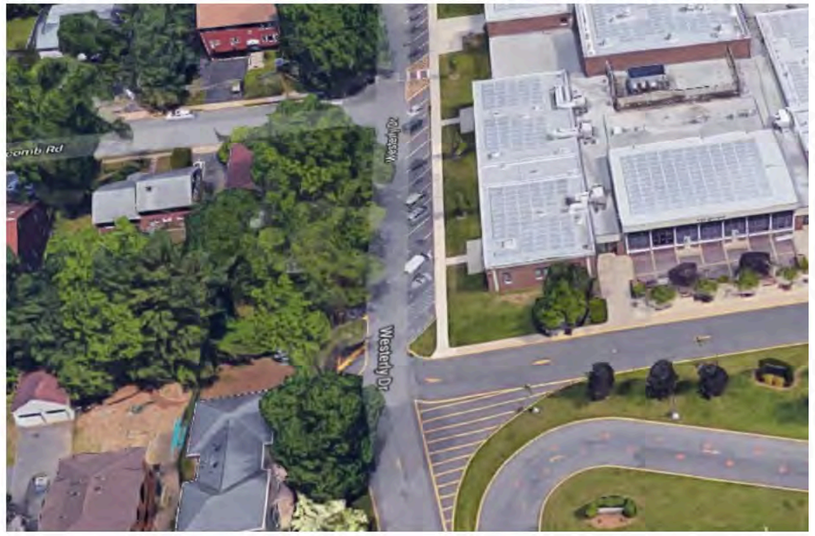
Lawrence Lasker, Walter F. Parkes


MISSILE WARNING
SUB-LAUNCH DETECTOR
Is it a game, or is it real?
WarGames

realism practicality Hollywood

Student Hacks High School, Changes Applications

By Catalin Cimpanu



Tenafly High School has informed parents earlier this mor
internal IT systems, changed grades to improve his GPA, a
after.

The New Jersey-based high school has not named the stud
enforcement is currently handling the investigation.

According to reports in local media [1, 2], the teen gained a
management system, and Naviance, a nationwide IT syste
grades, and other documents for the purpose of evaluating

NetHunter
https://www.kali.org/kali-linux-nethunter/

Los Angeles Times

CALIFORNIA

Riverside student hacks into school computers and changes grades, authorities say

A student is accused of tricking his teachers into sharing their personal computer login information by posing as a high-ranking administrative official. (Bill O'Leary / Washington Post)

By ALEXA DÍAZ | STAFF WRITER AUG. 5, 2019 | 11:44 AM

A Riverside high school student could face felony charges after authorities say he tricked his teachers into revealing their computer login information to polish his own grades and worsen others.

LATEST CALIFORNIA ›

CALIFORNIA
Public service, celebrations mark Martin Luther King Jr. holiday in L.A.
Jan. 19, 2020

CALIFORNIA
Number of bodies found buried in Tijuana home now up to 4
Jan. 19, 2020

CALIFORNIA
A baby gorilla is born at L.A. Zoo, the first in over 20 years
Jan. 19, 2020

CALIFORNIA
Family skeptical about integrity of San Diego State investigation into student's death
Jan. 19, 2020

CALIFORNIA
Suspect in killing of MMA gym owner dies after fight with fellow inmate, officials say
Jan. 19, 2020


MISSILE WARNING
SUB-LAUNCH DETECTION
Is it a game, or is it real?
WARGAMES

realismo praticabilità Hollywood

backdoor

A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers

Jargon File, 1981

SURVEILLANCE STATE —

Secret SSH backdoor in Fortinet hardware found in more products

Company warns customers to remove undocumented authentication feature ASAP.

DAN GOODIN - 1/22/2016, 9:30 PM

A recently identified backdoor in hardware sold by security company Fortinet has been f
several new products, many that were running current software, the company warned t

FURTHER READING

Et tu, Fortinet? Hard-codec
password raises new backd
eavesdropping fears

The undocumented account with a hard-coded password came to light last week when attack code exploiting the backdoor was posted online. In response, Fortinet officials said it affected only older versions of Fortinet's FortiOS software. The company went on to say the undocumented method for logging into servers using the s
shell (SSH) protocol was a "remote management" feature that had been removed in July

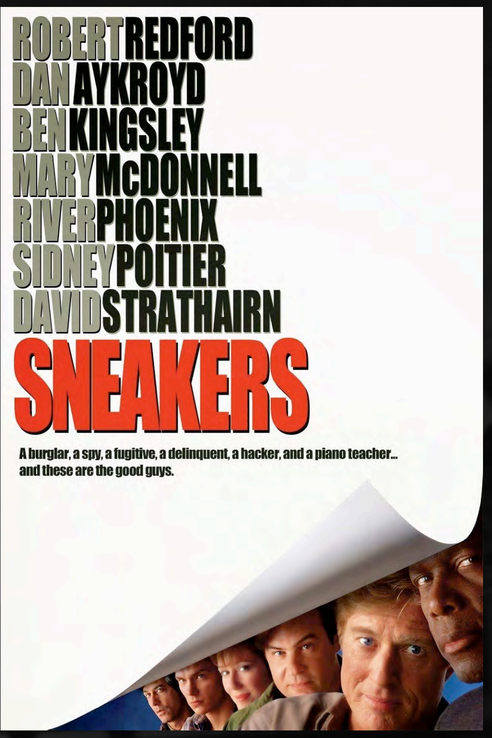
In a blog post published this week, Fortinet revised the statement to say the backdoor w
active in several current company products, including some versions of its FortiSwitch, FortiAnalyzer, and FortiCache devices. The company said it made the discovery after cor
review of its products. Company officials wrote:

> As previously stated, this vulnerability is an unintentional consequence of a feature was designed with the intent of providing seamless access from an authorized FortiManager to registered FortiGate devices. It is important to note, this is not a ca
> a malicious backdoor implemented to grant unauthorized user access.
>
> In accordance with responsible disclosure, today we have issued a security advisory provides a software update that eliminates this vulnerability in these products. This update also covers the legacy and end-of-life products listed above. We are actively working with customers and strongly recommend that all customers using the follo
> products update their systems with the highest priority:
>
> - FortiAnalyzer: 5.0.0 to 5.0.11 and 5.2.0 to 5.2.4 (branch 4.3 is not affected)

Backdoors Keep Appearing In Cisco's Routers

By Lucian Armasu July 19, 2018

Over the past few months, not one, not two, but five different backdoors joined the list of security flaws in Cisco routers.

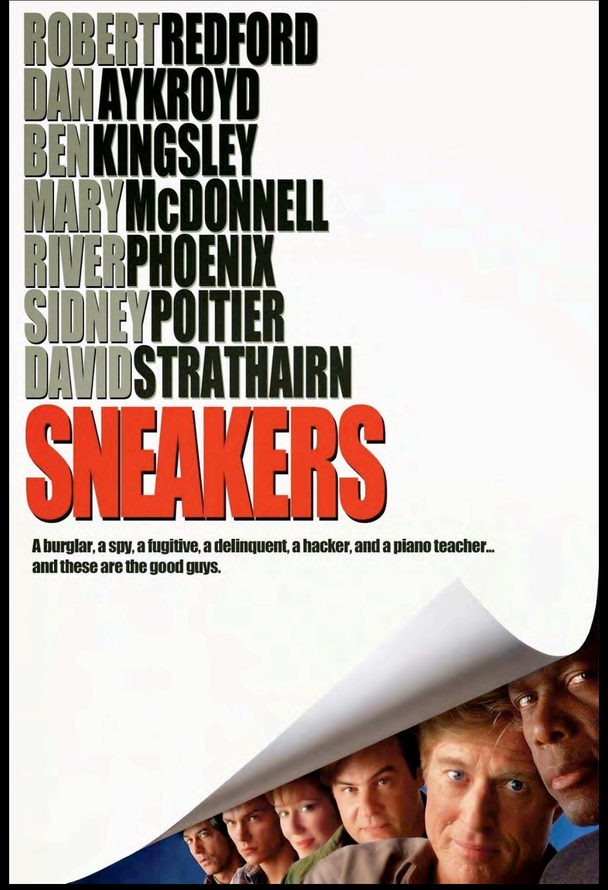


Sneakers, 1992

P.A.Robinson, L.Lasker, W.F.Parkes

SETEC ASTRONOMY


ROBERT REDFORD
DAN AYKROYD
BEN KINGSLEY
MARY McDONNELL
RIVER PHOENIX
SIDNEY POITIER
DAVID STRATHAIRN
SNEAKERS
a burglar, a spy, a fugitive, a delinquent, a hacker, and a piano teacher...
and these are the good guys.

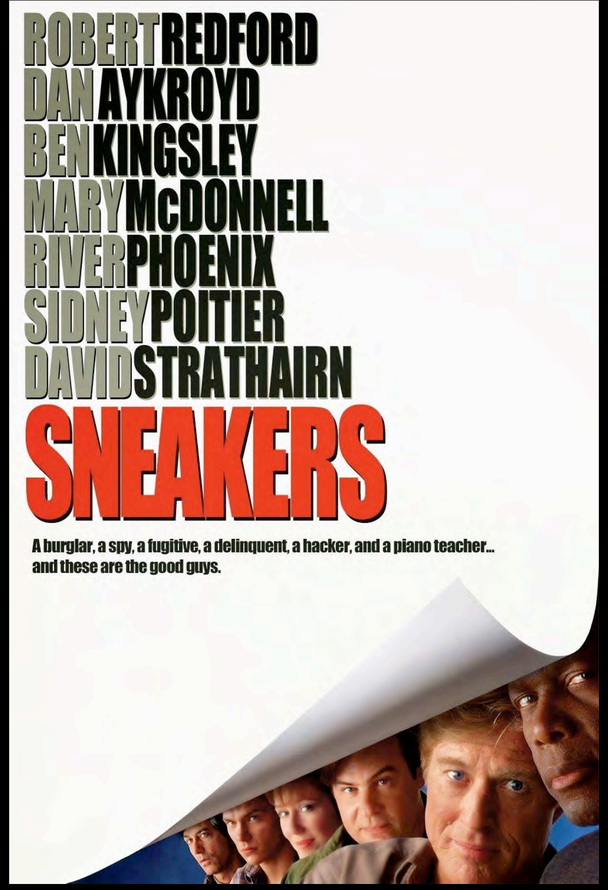


realism

practicality

Hollywood

ROBERT REDFORD
DAN AYKROYD
BEN KINGSLEY
MARY McDONNELL
RIVER PHOENIX
SIDNEY POITIER
DAVID STRATHAIRN
SNEAKERS
A burglar, a spy, a fugitive, a dellinquent, a hacker, and a piano teacher...
and these are the good guys.

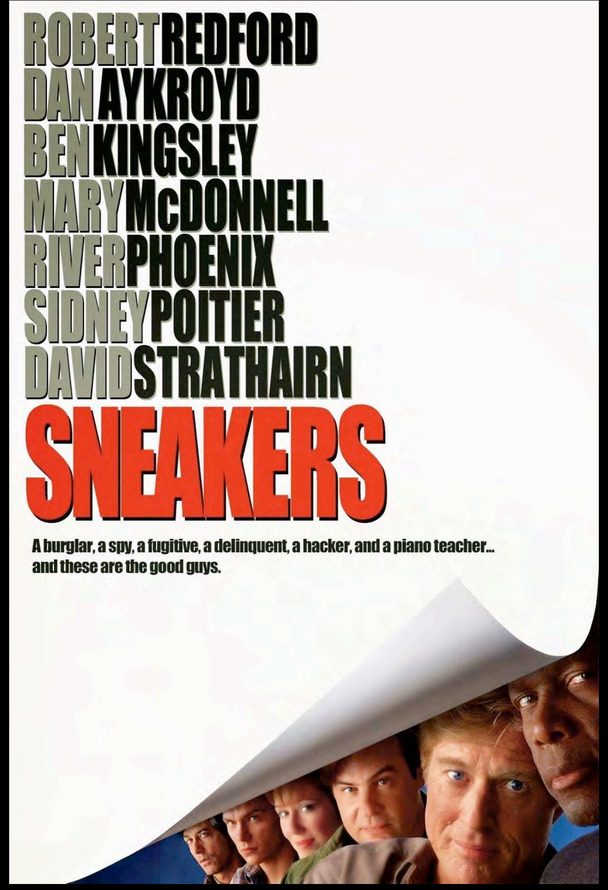


realismo

praticabilità

Hollywood

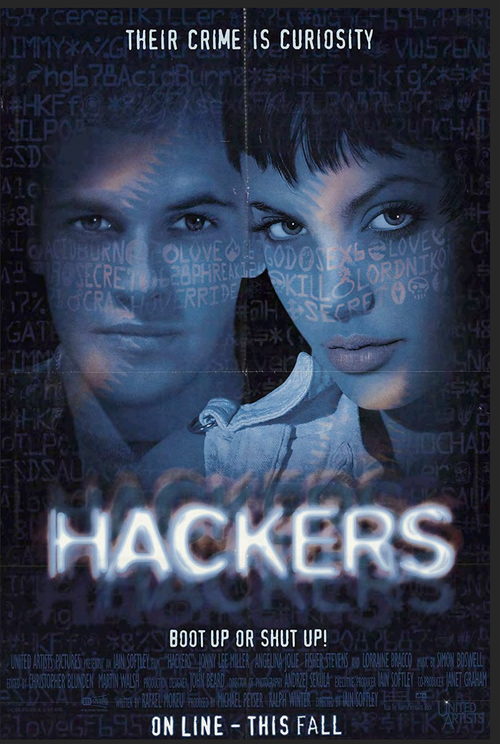

ROBERT REDFORD
DAN AYKROYD
BEN KINGSLEY
RIVER PHOENIX
SIDNEY POITIER
DAVID STRATHAIRN
SNEAKERS
A heister, a spy, a hustler, a millionaire, a hacker, and a piano teacher...
and these are the good guys.



realismo

praticabilita'

Hollywood



Hackers, 1995

Rafael Moreu

Garbage >

CONFIDENTIAL FILES

Do not delete before final backup is complete

FILE 1

waiting for backup

FILE 2

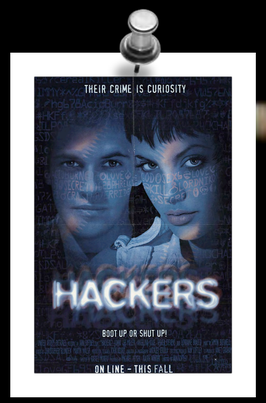
waiting for backup

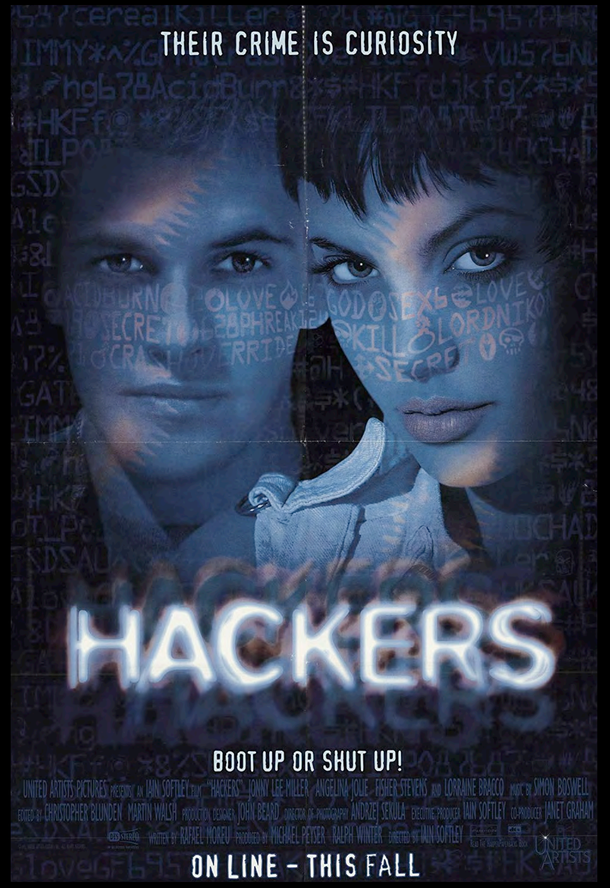
FILE 3

waiting for backup

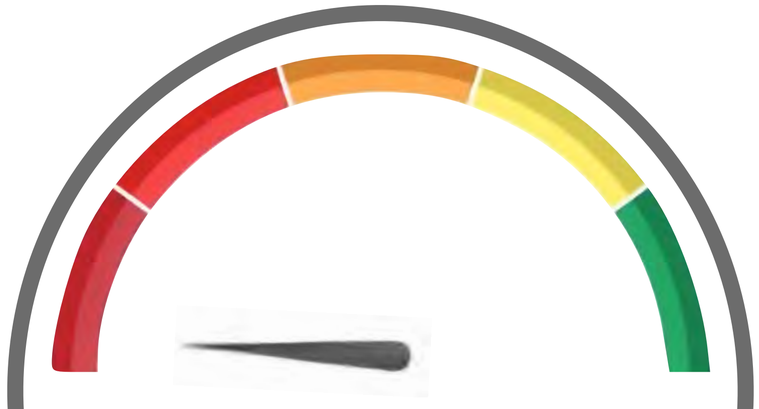
FILE 4

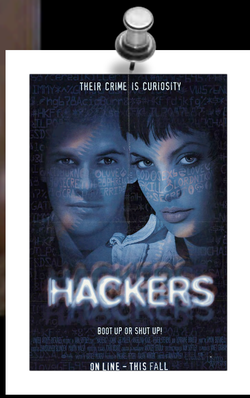
waiting for backup

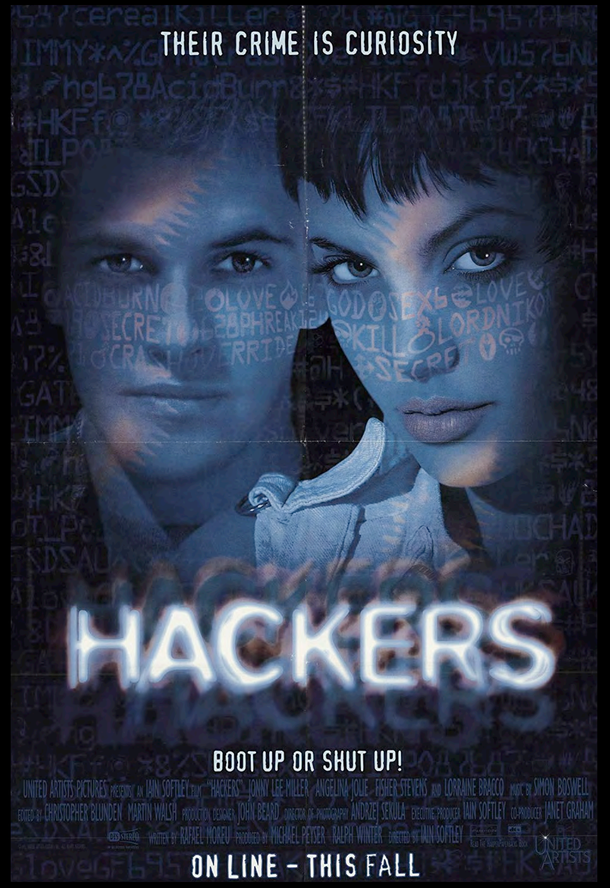

THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
ON LINE - THIS FALL



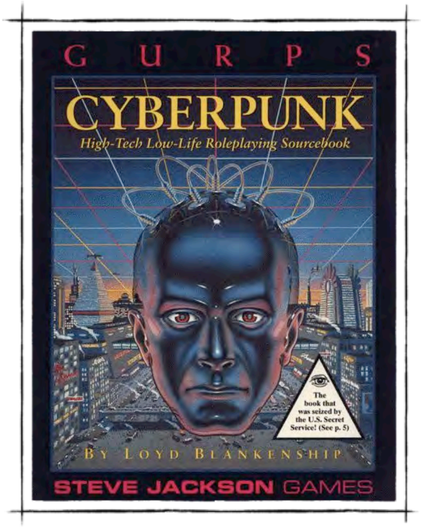
realism practicality Hollywood




THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
ON LINE - THIS FALL

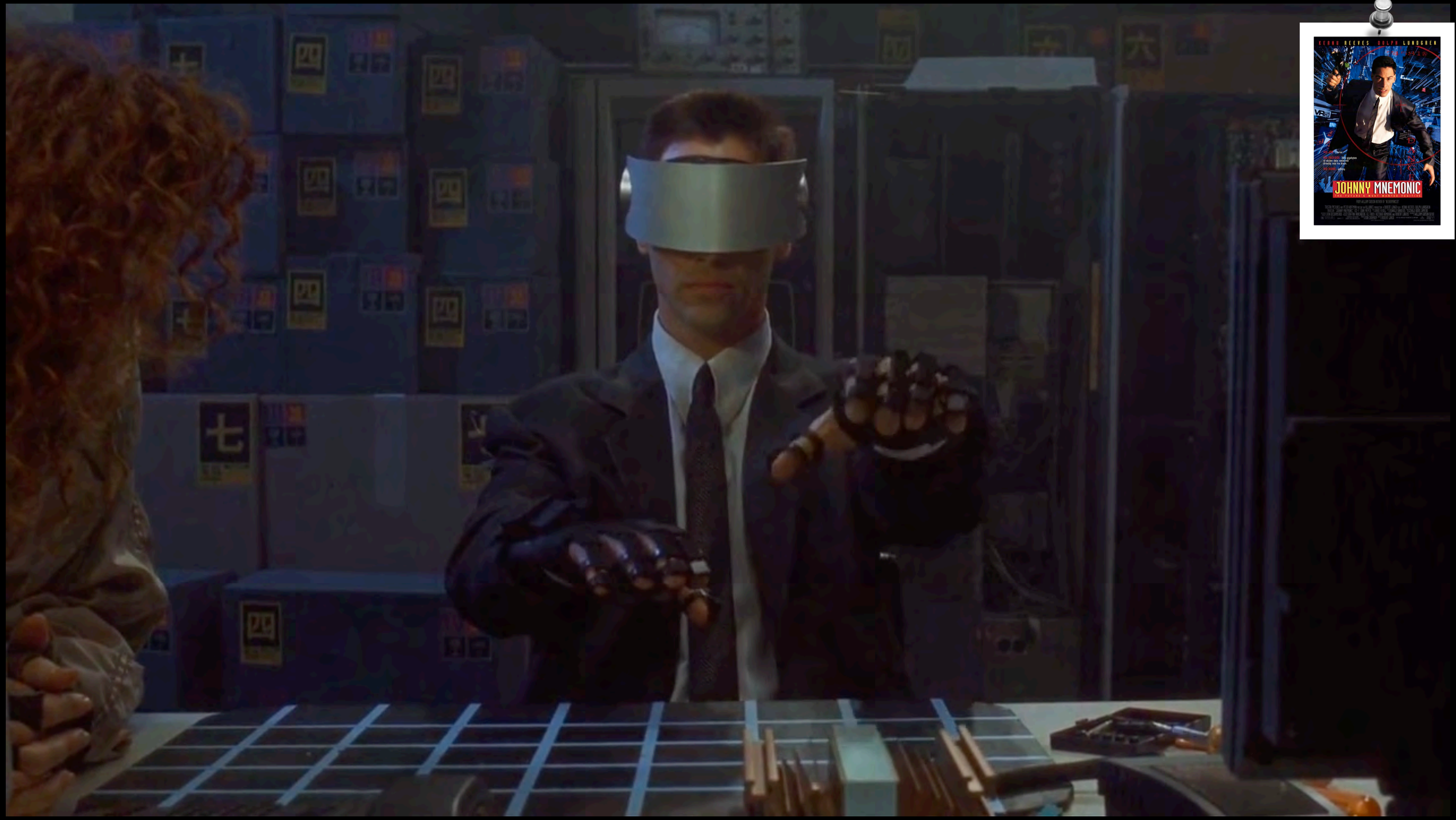


real:smo prat:cab:l:ta' Hol



Johnny Mnemonic, 1995

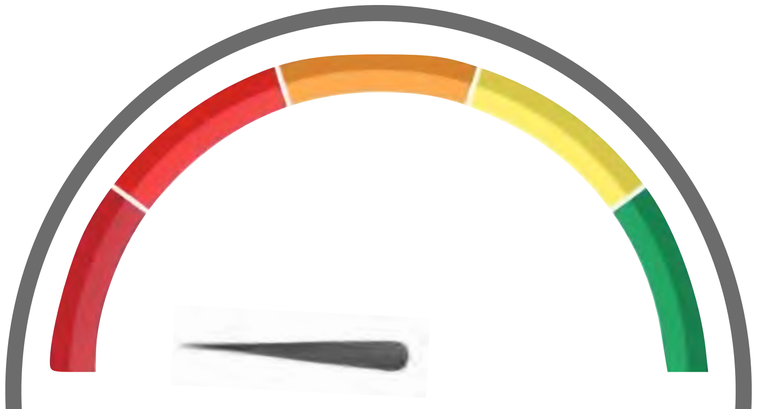
William Gibson

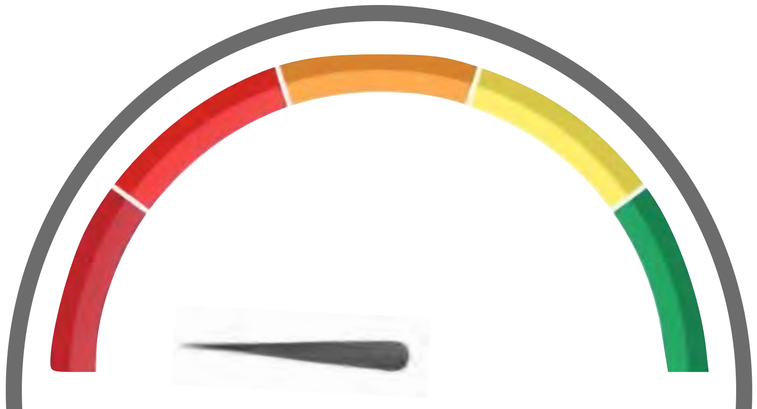

KEANU REEVES
DOLPH LUNDGREN
JOHNNY MNEMONIC

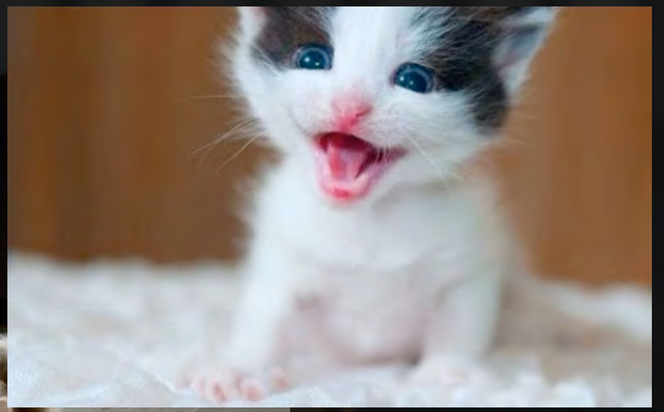
realismo

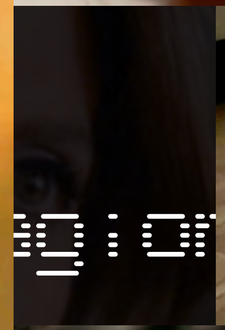
praticabilità

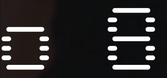
Hollywood



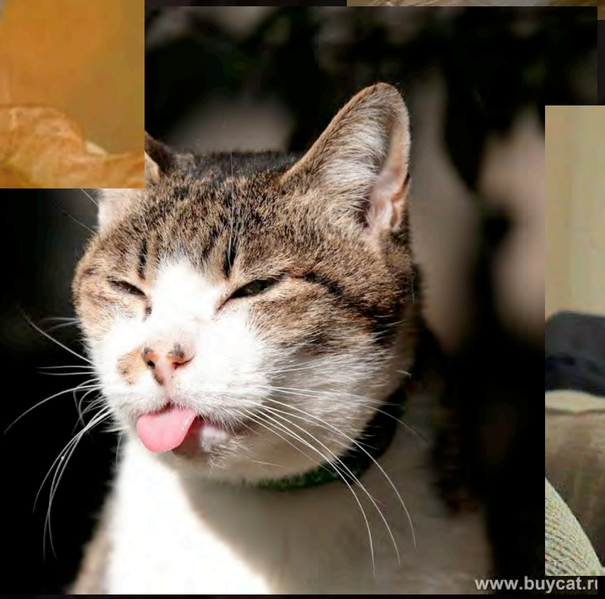




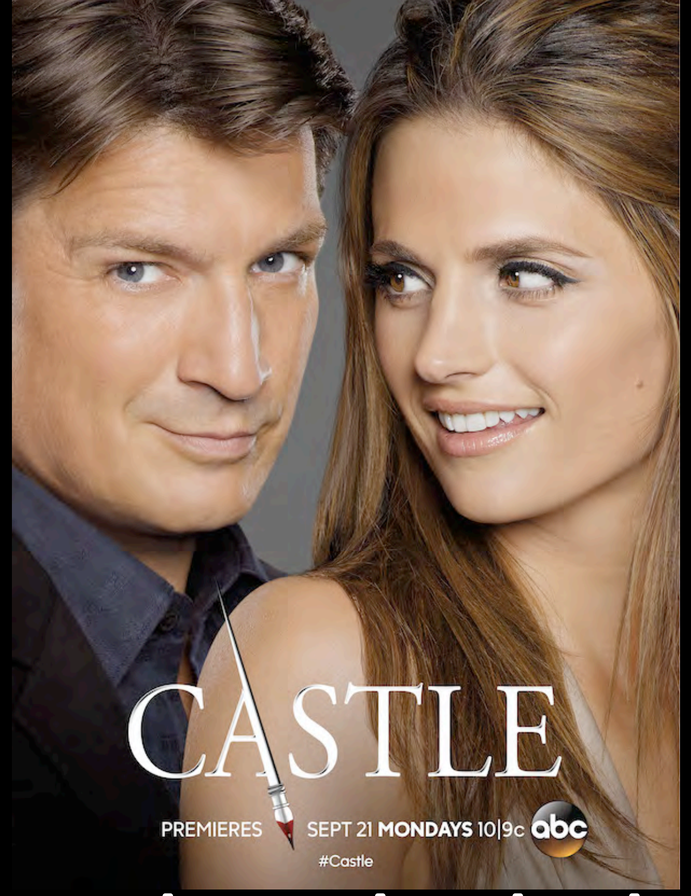




PREMIERES
SEPT 21 MONDAYS 10|9c abc
#Castle


www.buycat.ri

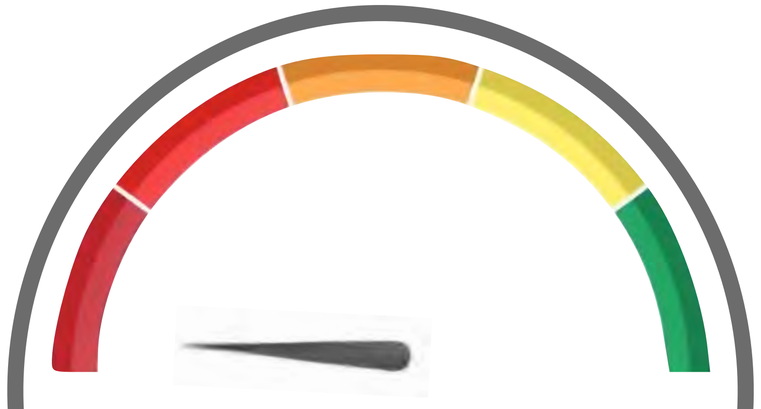

FIREWALL #4
Decrypting
14%
0%
FIREWALL #4
CASTLE
PREMIERES SEPT 21 MONDAYS 10/9c abc

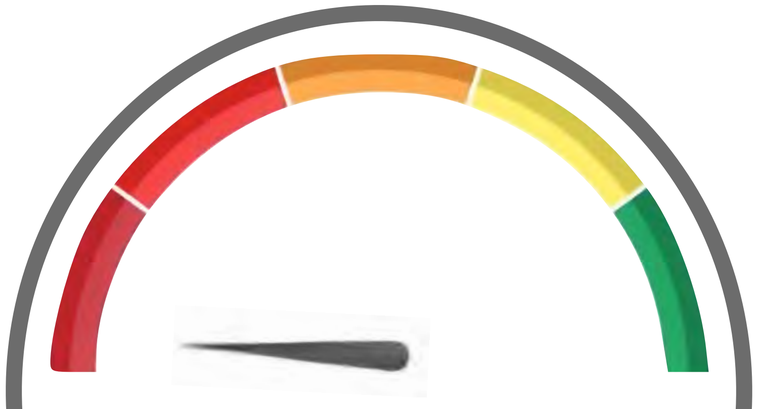


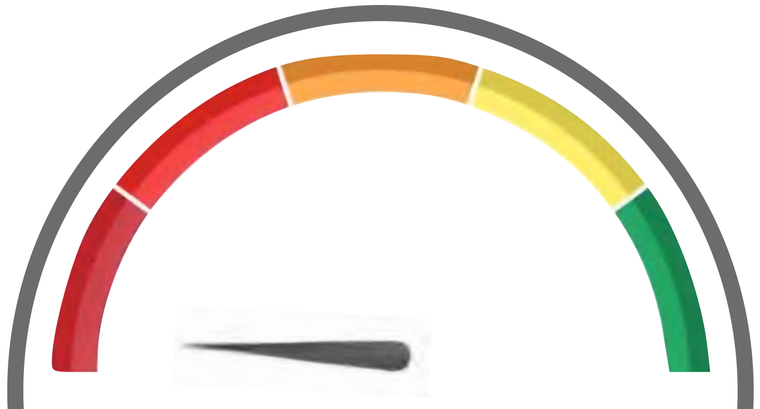
realismo

praticabilità

Hollywood







NCIS, Stagione 2 Episodio 5

double hacking

1995 BREAKING

FIREWALL CONNECTION BREACHE

USION DETECTION - FIREWALL BREAC

nRender[filename] userEntry

x?

n(shell) login....waiting...

rmote:hoist/dir[binhex] log???

arance = .00010.

> batchRender[filename] userEntry

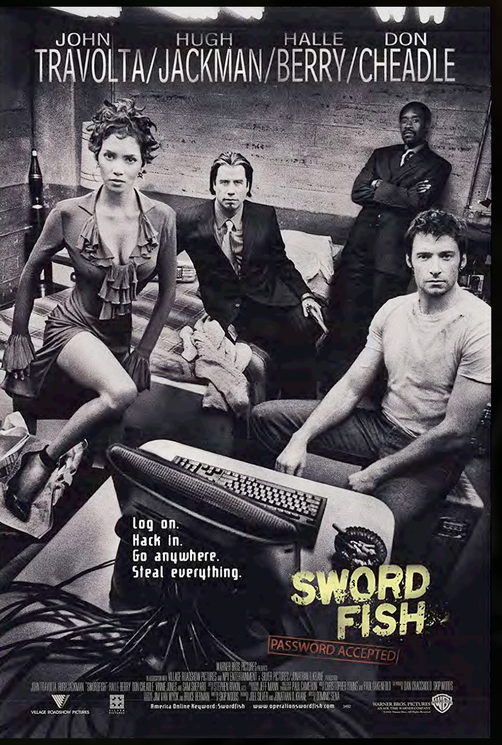
xxxxxx?

> open(shell) login....waiting...

> path:rmote:hoist/dir[binhex] log??

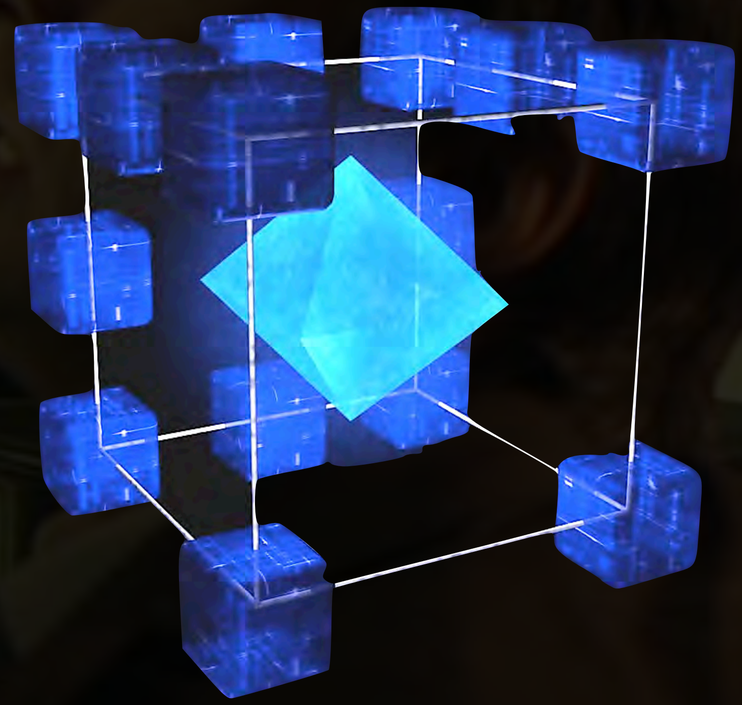
> tar/variance = .00010.

realismo praticabilità' Hollywood



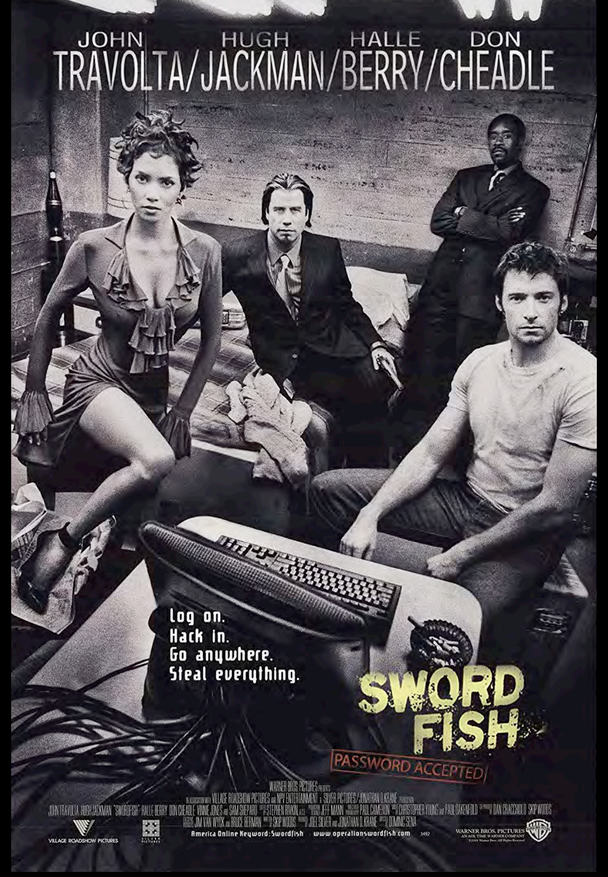
Swordfish, 2001

Skip Woods

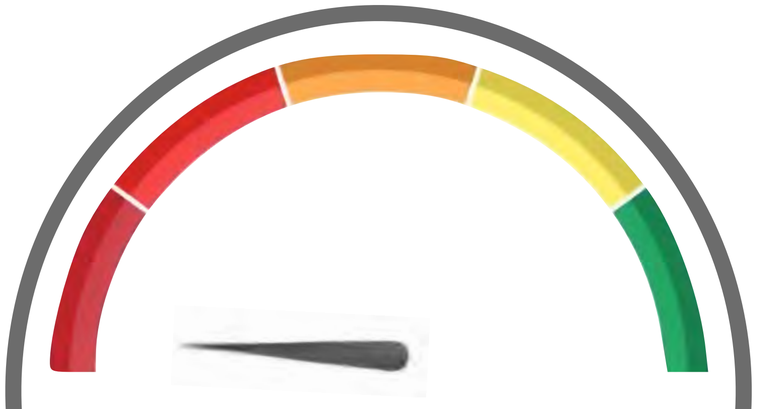


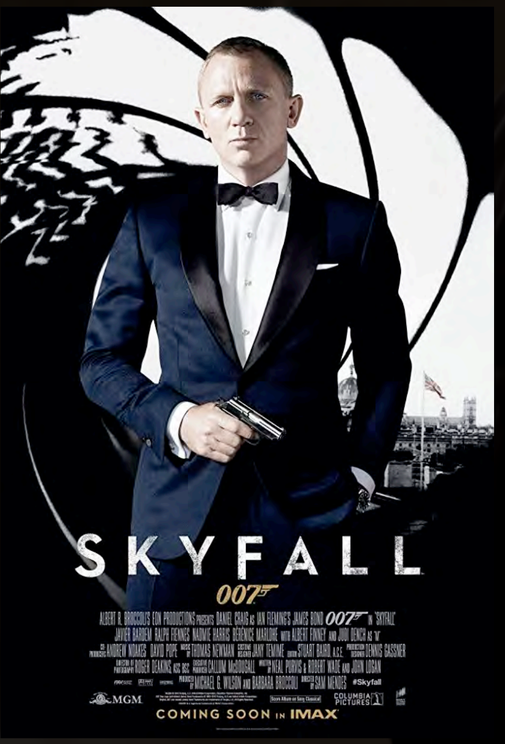

WORM GENERATOR TOOL V.1.2
IP ADDRESS PROTOCOL ROUTER SERVICE INTERRUPT QUERY
COMPILING OBJECTS
V.1.2 TOOL SET
INPUT ROUTING
LOCAL 1
LOCAL 2
SAT - AL42
SAT - J288
NETWORK A
NETWORK B
STRENGTH

JOHN TRAVOLTA
HUGH JACKMAN
HALLE BERRY
DON CHEADLE
SWORD FISH



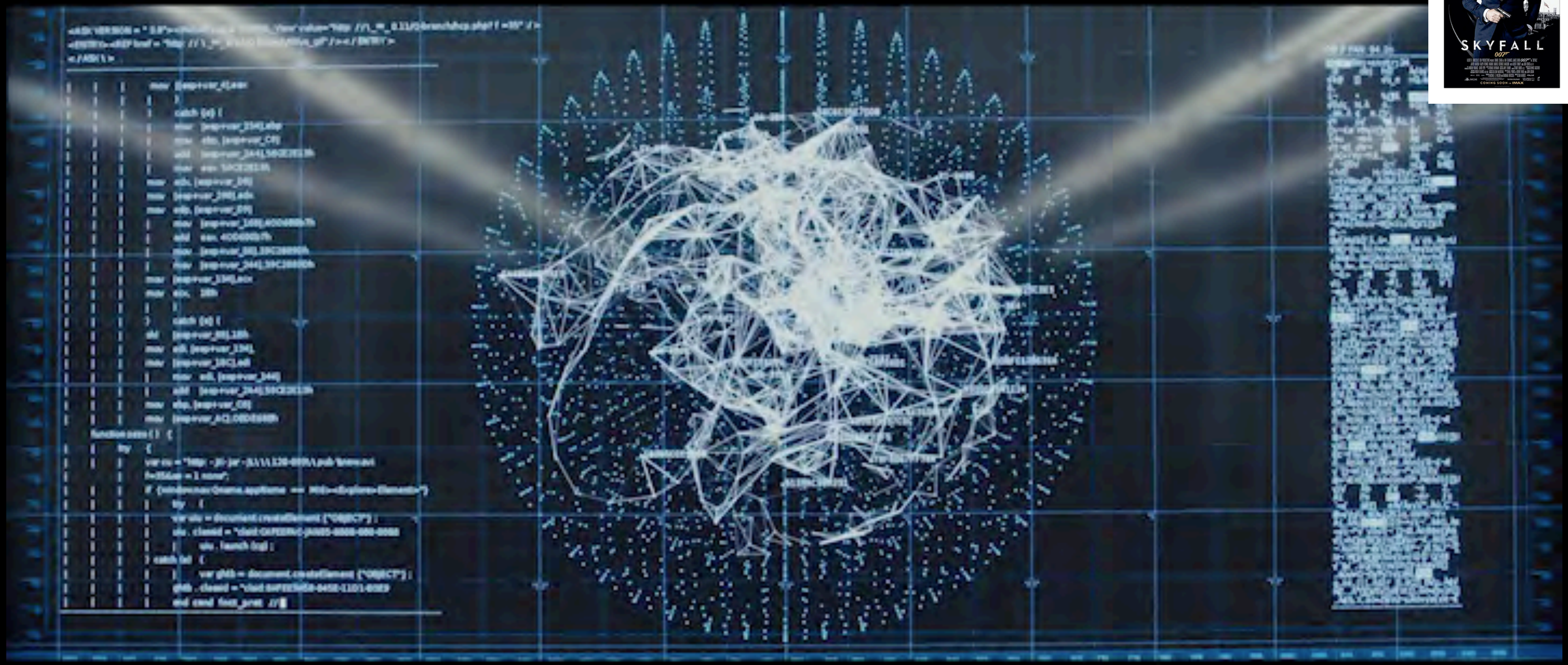
realismo probabilità Hollywood





Skyfall, 2012

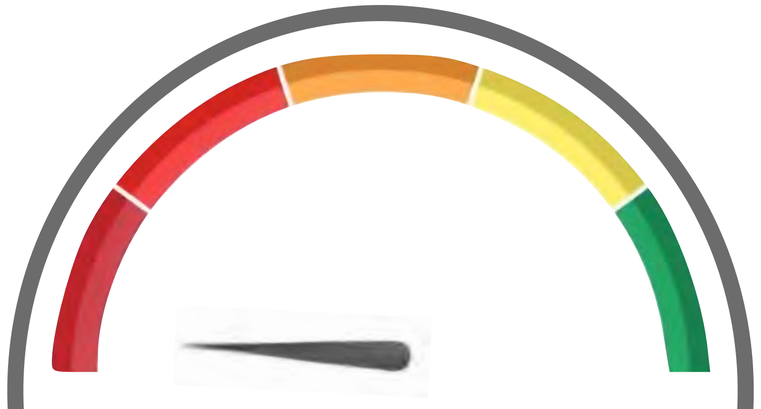
N.Purvis, R.Wade, J.Logan

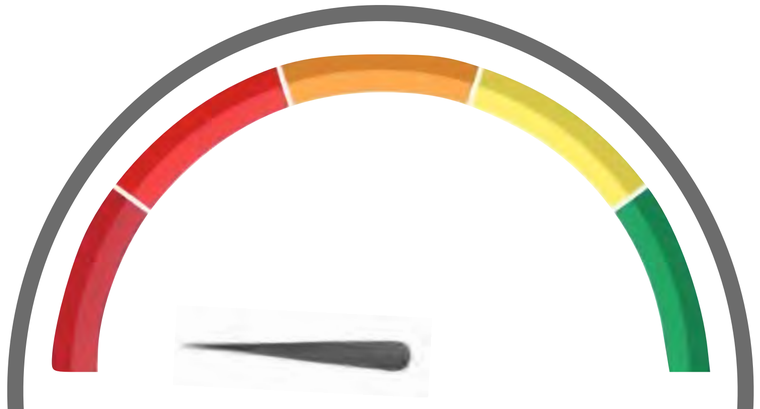

SKYFALL
007
COMING SOON to IMAX

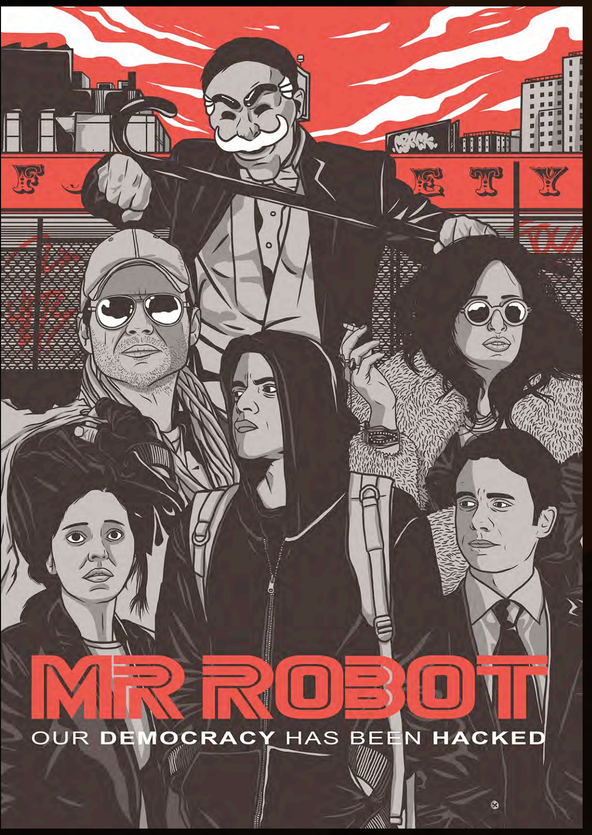
realismo

praticabilità

Hollywood





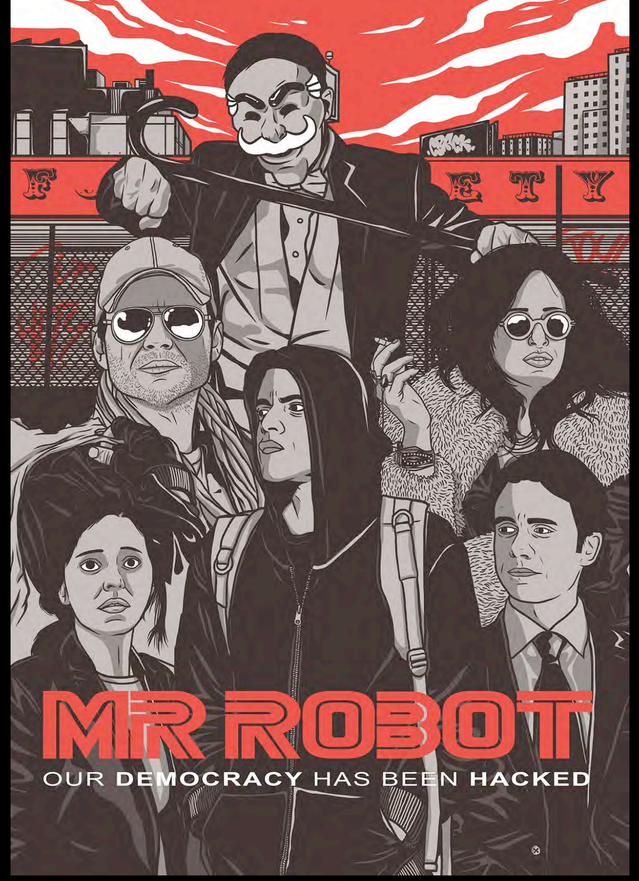


Mr.Robot
2015 - 2019

Sam Esmail


#MrRobot

MR ROBOT
OUR DEMOCRACY HAS BEEN HACKED

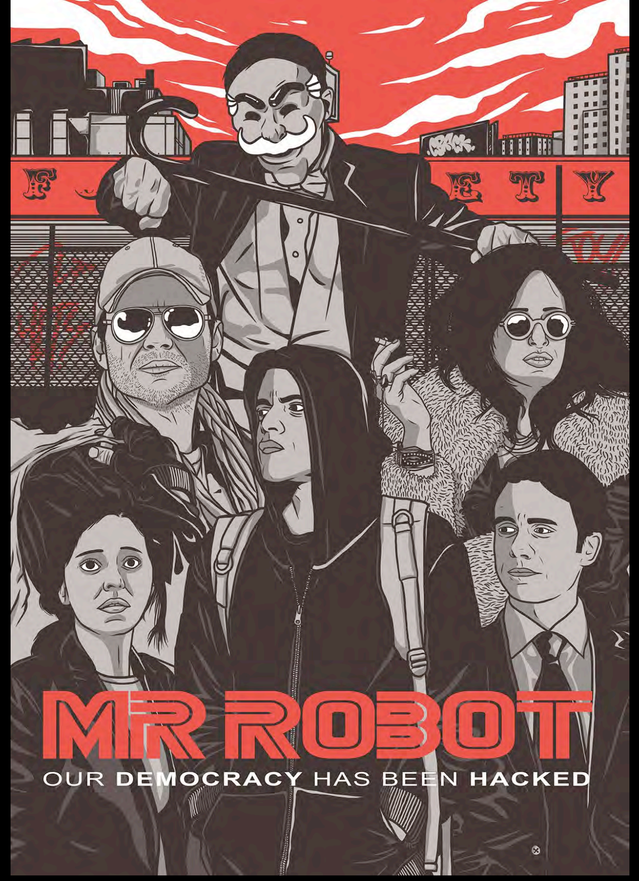


realismo

praticabilità

Hollywood

usa #MrRobot



realismo

praticabilità

Hollywood

USB Flash Drive Malware: How It Works & H

(3 votes, average: 4.33 out of 5)

FACEBOOK TWITTER

December 16, 2019

USB Flash Drive Ma to Protect Against It

From the University of Illinois USB flash drive malware is a

Back in 2016, researchers from the Univers around the University campus to see how p were found by students and staff, and the st device to try to access the content.

For a hacker trying to contaminate a compu paints a picture of how careless we can be

Let's hash it out.

A History of USB Drive Malware

BadUSB Malware Code Released — Turn USB Drives Into Undetectable CyberWeapons

October 04, 2014 Swati Khandelwal

Once again USB has come up as a major threat to a vast number of users who use USB drives – including USB sticks and keyboards. Security researchers have released a bunch of hacking tools that

Popular This Week

Microsoft Warns of Unpatched IE Browser Zero-Day That's Under Active Attacks

Saudi Prince Allegedly Hacked World's Richest Man Jeff Bezos Using WhatsApp

250 Million Microsoft Customer Support Records Exposed Online

Citrix Releases Patches for Critical ADC Vulnerability Under Active Attack

Broadening the Scope: A Comprehensive View of Pen Testing

USBHarpoon Is a BadUSB Attack with A Twist

August 20, 2018 05:54 PM 7

B charging cable, one that can compromise o a peripheral device capable of typing and

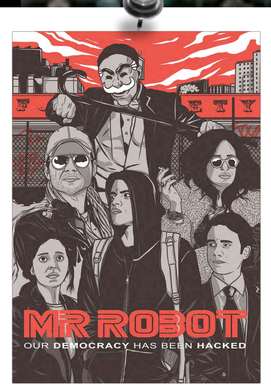
rch from Karsten Nohl and his team at an reprogram the controller chip of a USB e device (HID).

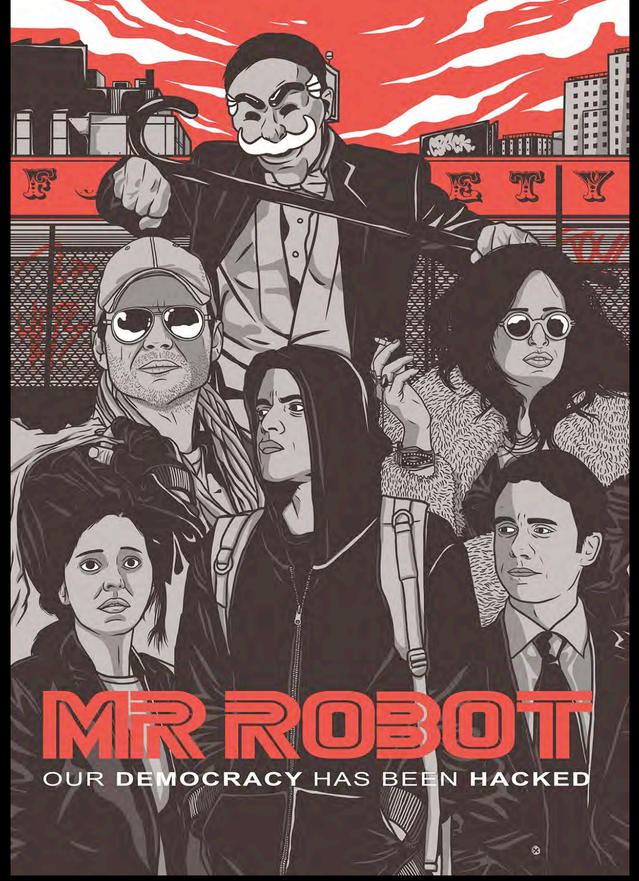
eyboard that issues a rapid succession of settings to redirect traffic.

ith a charging cable, something that is as

a and power to pass through so it will fulfill ed by any type of device that powers ut raising suspicions about plugging the

Behind the USBHarpoon project are Olaf Tan and Dennis Goh of RFID Research Group. Vincent Yiu of


MR ROBOT
OUR DEMOCRACY HAS BEEN HACKED

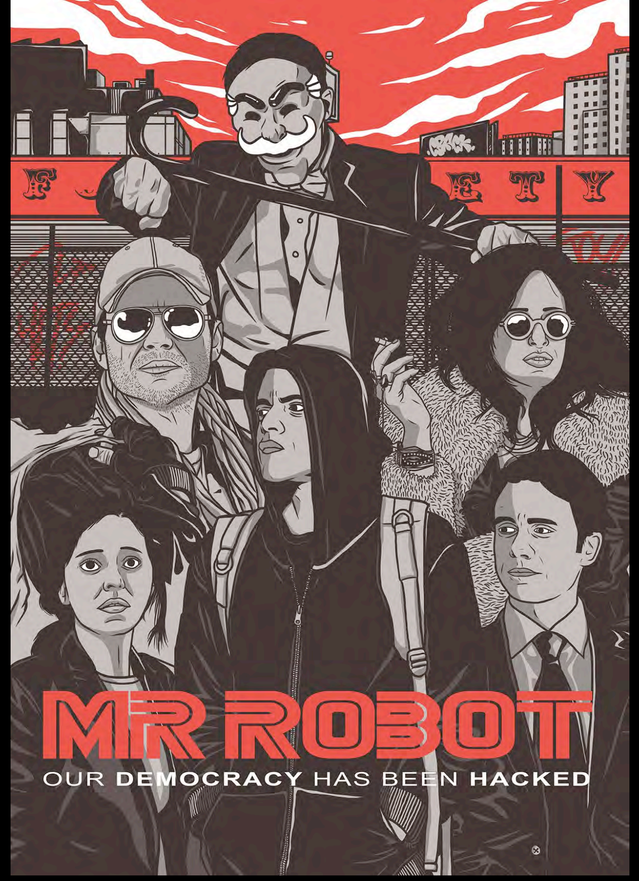


realismo

praticabilità

Hollywood

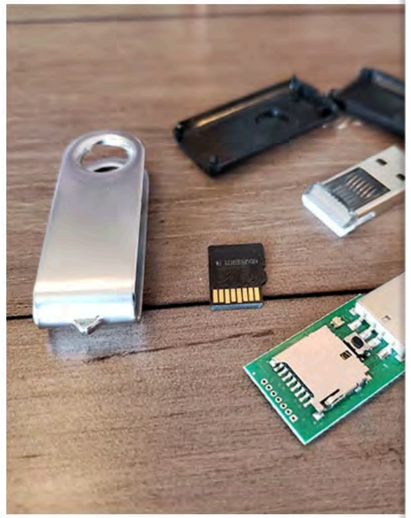

MR ROBOT
OUR DEMOCRACY HAS BEEN HACKED
usa



realismo

praticabilità

Hollywood



simple ducky payload.txt - Notepad

File Edit Format View Help

```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

INVERSE PATH | F-Secure

INDUSTRIES SERVICES **PRODUCTS** RESEARCH NEWS COMPANY

USB ARMORY **MK II** MK I

BUY NOW

OPEN SOURCE FLASH-DRIVE SIZED COMPUTER

The **USB armory** from **F-Secure** is an open source hardware design, implementing a flash drive sized computer.

The compact USB powered device provides a platform for developing and running a variety of applications.

The security features of the USB armory System on a Chip (SoC), combined with the openness of the board design, empower developers and users with a fully customizable USB trusted device for open and innovative personal security applications.

The hardware design features the NXP i.MX6UL processor, supporting advanced security features such as secure boot and ARM® TrustZone®.

The USB armory hardware is supported by standard software environments and requires very little customization effort. In fact vanilla Linux kernels and standard distributions run seamlessly on the tiny USB armory board.

- NXP i.MX6UL/i.MX6ULZ ARM® Cortex™-A7 900Mhz, 512MB/1GB DDR3 RAM
- USB host powered (<500 mA) device with compact form factor (65 x 19 x 6 mm)
- ARM® TrustZone®, secure boot + storage + RAM
- Secure elements Microchip ATECC608A and NXP A71CH
- internal 16GB eMMC + external microSD
- u-blox ANNA-B112 Bluetooth module
- debug accessory support for UART, GPIO, SPI, I²C, CAN breakout
- customizable LEDs, including secure mode detection
- supported by vanilla Linux kernels and distros
- USB device emulation (CDC Ethernet, mass storage, HID, etc.)
- Open Hardware & Software

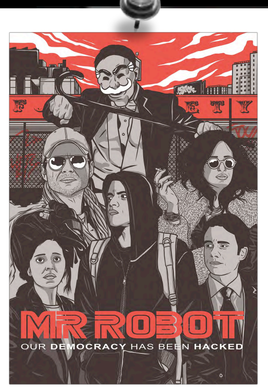
APPLICATIONS

The USB armory board has been created to support the development of a variety of security applications.

The capability of emulating arbitrary USB devices in combination with the i.MX6UL SoC speed, the security features and the

The following example security application ideas illustrate the flexibility of the USB armory concept:

- Hardware Security Module (HSM)
- encrypted file storage with malware scanning, host


MR ROBOT
OUR DEMOCRACY HAS BEEN HACKED

Security

Hackers clone pl

"You shou

By Jack Clark in

Black Hat 201
use of femtoce
femtocell, allo
nearby mobile

The exploit wa
Vegas after be
by Verizon and
already been r

Femtocells are
reach places,
themselves an

DIY

How To Make a Wi-Fi Antenna Out Of a Pringles Can

By Ian Buckley / February 3, 2017 / 10 minutes

Affiliate Disclosure: By buying the products we recommend, you help keep the site alive. Read more.

DIY solutions to extending Wi-Fi have existed for as long as Wi-Fi itself has. Ingenious internet users have been using everything from kitchen foil and food strainers, to home made Yagi style antennas to boost their Wi-Fi ranges. While there are many ways you can fine tune your home Wi-Fi system without building additional hardware, there are simple DIY solutions that can also make a real difference to your surfing experience.

Improve Your Wi-Fi Signal at Home & Outside with These Android Apps

Looking to improve the Wi-Fi signal in your home or find a Wi-Fi connection when you're out? This article has you covered.

READ MORE

Before you start though, make sure you have checked whether you have any other problems with your Wi-Fi connection.

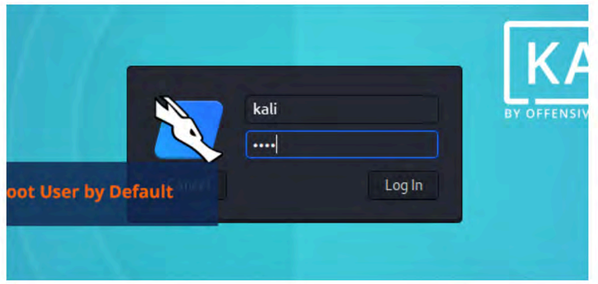
Meet the $250 Verizon device that

KALI BY OFFENSIVE SECURITY

Blog Downloads Training Documentation Community About Us

Our Most Advanced Penetration Testing Distribution, Ever.

Latest Kali Linux News and Tutorials



Kali Default Non-Root User

December 31, 2019 elwood Kali Linux News

For years now, Kali has inherited the default root user policy from BackTrack. As part of our evaluation of Kali tools and policies we have decided to change this and move Kali to a "traditional default non-root user" model. This change will be part of the 2020.1 release, currently scheduled for late January. However, you will notice this change in the weekly images starting now.

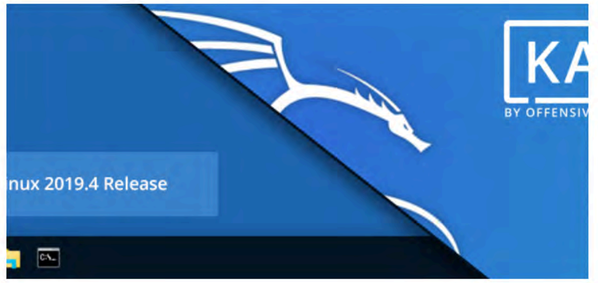
READ MORE

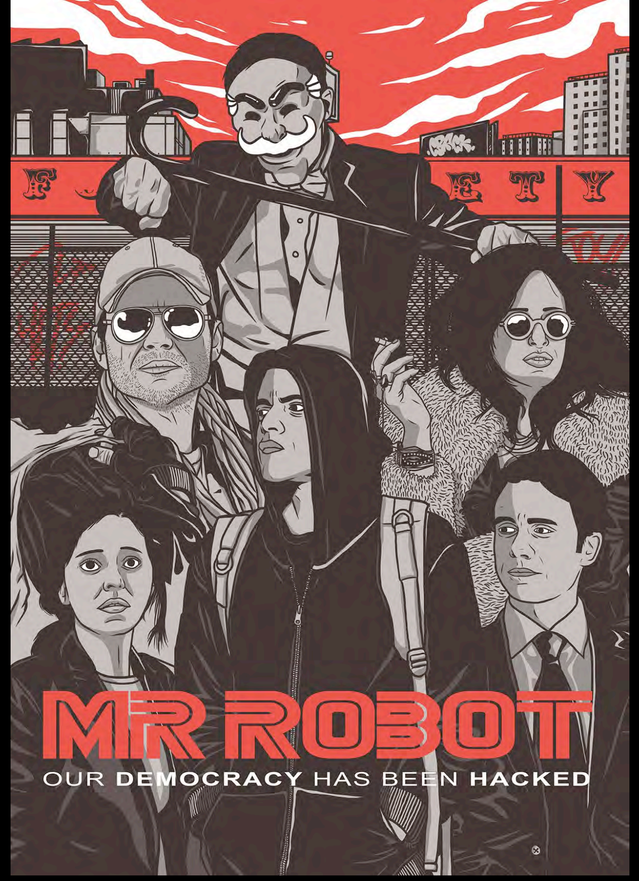
How Kali deals with the upcoming Python 2 End-of-Life

December 16, 2019 elwood Kali Linux News

Five years ago, the Python developers announced that they will stop supporting Python 2 in 2020. For a long time, nobody cared and Python 3 adoption was slow. But things have changed a lot lately as the deadline is right around the corner (1st January).

READ MORE





realismo

praticabilità

Hollywood

Who Am I
Kein System
ist sicher, 2014
J.Friese, B.bo Ordar


NO SYSTEM IS SAFE
WHO AM I
A FILM BY BARAN BO ODAR

realismo

praticabilità

Hollywood

NO SYSTEM IS SAFE
WHO AM I
A FILM BY BENJAMIN RO OHAM
tiff.

realismo praticabilita' Hollywood

Blackhat, 2015

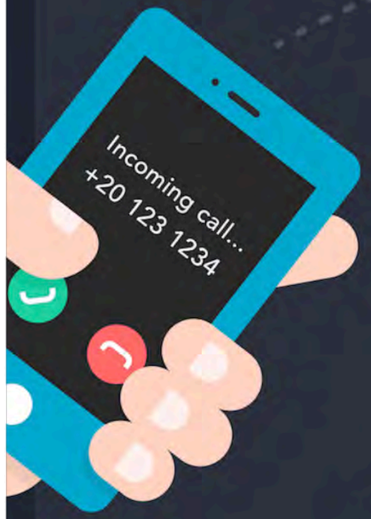
Morgan Davis Foehl

To: r.donahue@secure.nsa01.gov
From: b.hitchens@secure.nsa01.gov
Subject: Revised draft of intelligence report
Received: Today

realismo praticabilità Hollywood

5 Next year, nearly half of phone calls will be scams.

Percentage of spam calls in the United States*

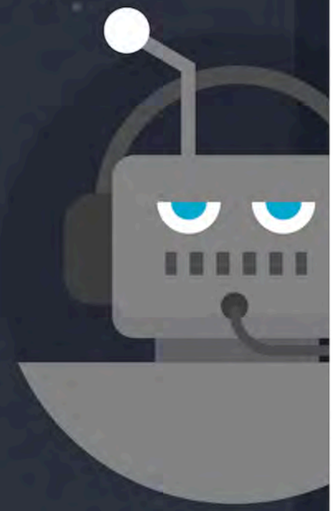


2017

29%

2018

45%



*According to First Onion

2 Cyber attackers now mainly prey on enterprises.

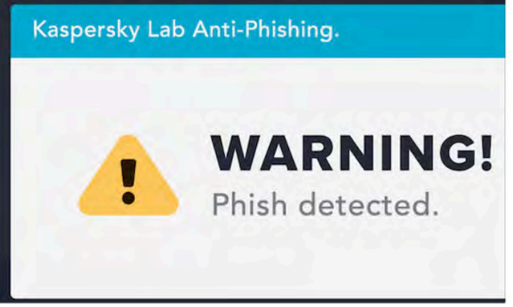
2017

76% of businesses were victims of phishing attacks.

Kaspersky Lab's Anti-Phishing system was triggered

246,231,645

times in 2017.



Snowden, 2016

K.Fitzgerald, O.Stone

realismo praticabilità Hollywood

theguardi

MICROSOFT | POLICY | US & WORLD

Microsoft labels US gove threat' in plan to cut off

By Tom Warren | @tomwarren | Dec 5, 2013, 3:36am EST

Source Microsoft Fire Hose

SHARE

microsoft logo granite stock 1020

Microsoft is unveiling an aggressive plan today to combat g
Smith, Microsoft's general counsel, says the software giant
customers about government surveillance of the internet, a
with improved encryption, legal protections, and source co
blog post, Smith labels government snooping an "advanced
generally used to describe teams of hackers that coordinat
governments.

Microsoft's response follows recent revelations that the NSA

Schneier on Security

Blog >

NSA Eavesdropping on Google and Yahoo Networks

The *Washington Post* reported that the NSA is eavesdropping on the Google and Yahoo private networks -- the code name for the program is MUSCULAR. I may write more about this later, but I have some initial comments:

- It's a measure of how far off the rails the NSA has gone that it's taking its Cold War–era eavesdropping tactics -- surreptitiously eavesdropping on foreign networks -- and applying them to US corporations. It's skirting US law by targeting the portion of these corporate networks outside the US. It's the same sort of legal argument the NSA used to justify collecting address books and buddy lists worldwide.
- Although the *Washington Post* article specifically talks about Google and Yahoo, you have to assume that all the other major -- and many of the minor -- cloud services are compromised this same way. That means Microsoft, Apple, Facebook, Twitter, MySpace, Badoo, Dropbox, and on and on and on.
- It is well worth re-reading all the government denials about bulk collection and direct access after PRISM was exposed. It seems that it's impossible to get the truth out of the NSA. Its carefully worded denials always seem to hide what's really going on.
- In light of this, PRISM is really just insurance: a way for the NSA to get legal cover for information it already has. My guess is that the NSA collects the vast majority of its data surreptitiously, using programs such as these. Then, when it has to share the information with the FBI or other organizations, it gets it again through a more public program like PRISM.
- What this really shows is how robust the surveillance state is, and how hard it will be to craft laws reining in the NSA. All the bills being discussed so far only address portions of the problem: specific programs or specific legal justifications. But the NSA's surveillance infrastructure is much more robust than that. It has many ways into our data, and all sorts of tricks to get around the law. Note this quote from yesterday's story:

> John Schindler, a former NSA chief analyst and frequent defender who teaches at the Naval War College, said it is obvious why the agency would prefer to avoid

About Bruce Schneier

I am a public-interest technologist, working at the intersection of security, technology, and people. I've been writing about security issues on my blog since 2004, and in my monthly newsletter since 1998. I'm a fellow and lecturer at Harvard's Kennedy School and a board member of EFF. This personal website expresses the opinions of neither of those organizations.

Related Entries

NSA Spied on Prominent Muslim

ction program

ies to a wide range of digital information, including
t does not require individual warrants. Instead, it
illance Act (FISA). Some documents describing the
onal details about how the program operates,
ogram interacts with the Internet companies. These
Read related article.

Who holds top-secret security clearances? »

gram collects from the fiber-optic cable networks
ect North America to the rest of the world.