

# Sicurezza Informatica

Dr. Marco Balduzzi

Myself

Discussion:

Sono il primo!!!

(too old to reply)

**./SuperbepS**

15 years ago

A scrivere nella nuova mailing list!!!

- --=20

Ciao ???

**embyte**

----BEGIN PGP SIGNED MESSAGE----

Hash: SHA1

A scrivere nella nuova mailing list!!!

grrr mi hai fregato :p

--=20

/\" ASCII RIBBON CAMPAIGN=0D

\ / AGAINST HTML MAIL=0D

X BGLUG member @ bglug.linux.it =0D

/ \ Rawlab member @ rawlab.cjb.net=0D

\ / =C2=A7 embyte =C2=A7 ICQ UIN #48790142=0D

=0D

PGP KEY @ <http://web.tiscali.it/embyte/pgpkey/embyte.asc>=0D

=0D

"I videogames non influenzano i bambini: infatti se da piccoli=0D  
fossimo stati plagiati da Pac-Man, adesso passeremmo il nostro tempo=0D  
in ambienti semibui, mangiando pillole magiche ed ascoltando della=0D  
musica elettronica ripetitiva." Kristian Wilson, Nintendo Inc, 1989=0D



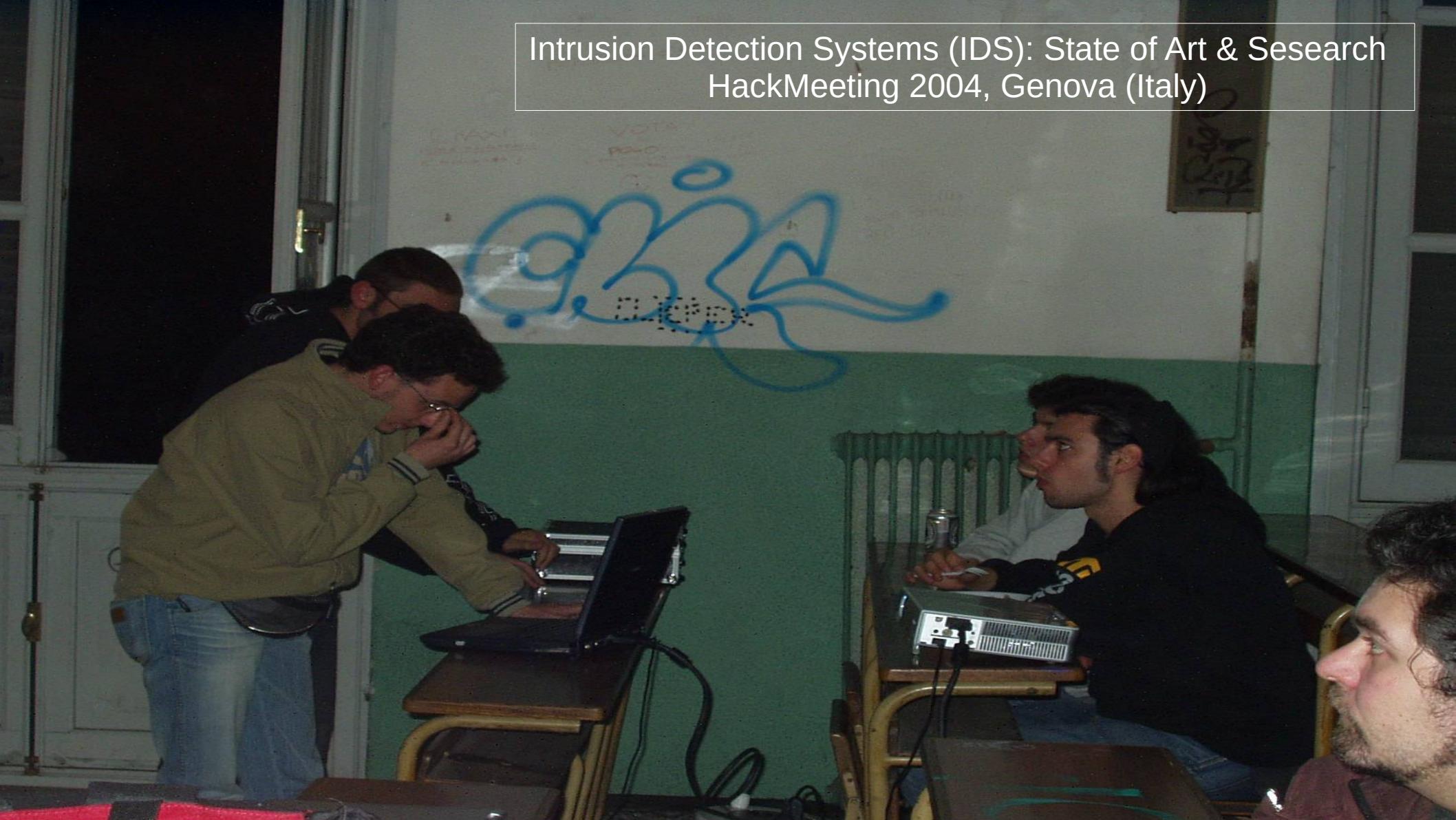
BGLUG



HackMeeting 2003, Torino (Italy)



Intrusion Detection Systems (IDS): State of Art & Sesearch  
HackMeeting 2004, Genova (Italy)



# Researchers Find Amazon Cloud Servers Teeming With Backdoors And Other People's Data



**Andy Greenberg** Former Staff

Security

Covering the worlds of data security, privacy and hacker culture.

Follow

⌚ This article is more than 9 years old.

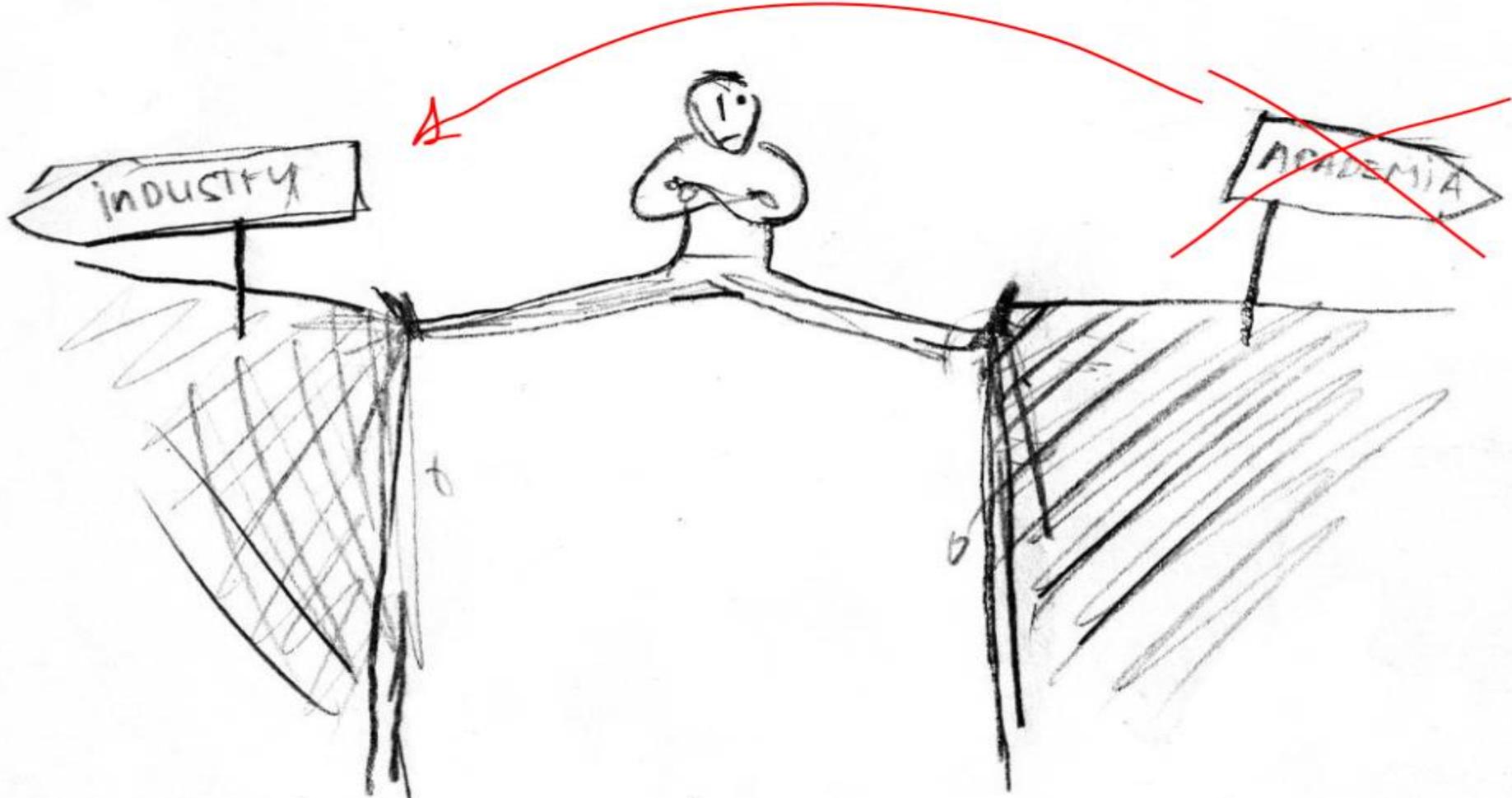
f Renting a server from Amazon Web Services promises all the advantages of the Cloud: ephemeral, convenient computing without the nuisance of owning hardware. In fact, it may be more like renting a house where the last tenant left his junk in the closets and hasn't changed the locks.



Eurecom's researchers (from the left) Jonas Zaddach, Davide Balzarotti, and Marco Balduzzi

Researchers at France's Eurecom technology institute, Northeastern University and the security firm SecluID ran automated scanning tools on more than 5,000 of the virtual machines images published on Amazon's catalog of virtual machines set up with preset software and configurations and ready to run on Amazon's Elastic Compute Cloud (EC2) service. They looked for security and privacy issues like malware, software









## TECNOLOGIA

## Dark web, tra droghe e falsi vaccini contro il coronavirus: il podcast

14 gen 2021 - 18:02

Alberto Giuffrè

**C**i sono criminali che vendono qualsiasi cosa, dalla droga ai passaporti falsi. E c'è anche chi prova a piazzare presunte dosi di vaccino contro il coronavirus. E' il dark web, quella parte dell'Internet nascosta ai motori di ricerca. Ne parliamo in questa puntata di 1234

CONDIVIDI: [f](#) [t](#) [f](#)

Si chiamava "Berlusconi market" ma con l'ex presidente del Consiglio non aveva nulla a che vedere. Era una delle più grandi piazze di spaccio del dark web, gestita da tre italiani da poco condannati a quattro anni di carcere. Da qui parte la nuova puntata di 1234, il [podcast](#) sulla sicurezza informatica di SkyTg24.

### Deep web e Dark web

Il dark web è una parte del deep web, cioè di quel mondo di siti internet nascosti ai motori di ricerca. Il dark web si appoggia a reti chiuse e ospita nella stragrande maggioranza attività illecite come appunto i mercati dove trovare qualsiasi cosa. A spiegarci come funziona e quali insidie nasconde è l'esperto Marco Balduzzi, ricercatore di Trend Micro.



★★★★★

12 reviews | Write a review

\$600.00

Ex Tax: \$600.00

Product Code: Passport  
Stock  Instock

### OVERVIEW

Italian original quality biometric passport for sale. Model 2021 year. Valid for 10 years after issuance (for adults over 18). The younger holders have document with 5 years validity. New version of the passport contains 48 pages. This document can ...

QTY 1

ADD TO CART



Pistol CZ Tactical with collimator, 9x19  
Price: €1100=\$0.1639



CZ SP-01 Shadow duotone 9 mm Luger  
Price: €700=\$0.1043



Beretta90TW 9mm  
Price: €800=\$0.1192



GL42 IV kal.380 AUTO  
Price: €500=\$0.0745



Sniper Rifle Mauser k-98,optics Hensoldt Wetzlar  
Price: €1800=\$0.2682



P08 American Eagle cal. 9  
Price: €800=\$0.1192

# Sistemi Ais vulnerabili, 400mila navi a rischio

Sistemi di identificazione automatica vulnerabili a una vasta gamma di attacchi. Ecco come gli hacker spiazzano la navigazione alterando i dati sulle rotte e creando imbarcazioni fantasma  
di Patrizia Licata



Navi a rischio pirateria informatica: nell'era della **Internet** delle cose il pericolo è più che mai attuale se le comunicazioni vengono affidate a sistemi non troppo sicuri. Durante la **HITB Security Conference** che si è tenuta la scorsa

settimana a Kuala Lumpur, i ricercatori del Forward Looking Threat di **Trend Micro** hanno dimostrato come i sistemi di identificazione automatica (**Ais**) oggi usati dalle navi siano vulnerabili a una vasta gamma di attacchi facilmente realizzabili da pirati, terroristi o altri criminali.

Attack 3: CPA Alerting [1/2]

- Fake a CPA alert (Closest Point of Approach) and trigger a collision warning alert.

net-security.org

# Hackers in Italy take over remote crane controls and operate cranes

by Crane Market | Jan 15, 2019 | Construction & Business News, Crane & Lifting News, Equipment & Construction Videos

-----

## Sicurezza: fallo nei macchinari industriali, a rischio cantieri, fabbriche e logistica

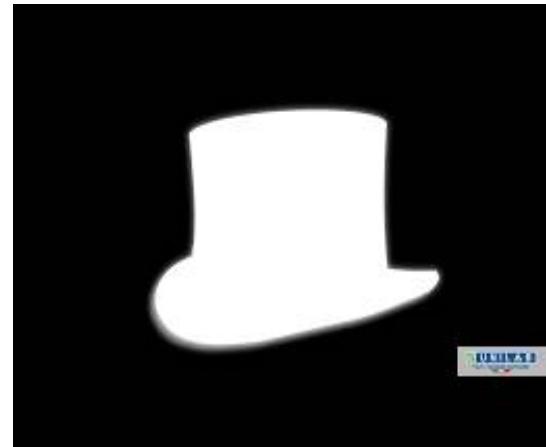
5 Febbraio 2019



Construction sites across the world are at risk of being shut down and extorted by hackers, cybersecurity researchers Federico Maggi and Marco Balduzzi warned. They hacked into real life cranes across sites in Italy.FEDERICO MAGGI

# Underground Community

# Black Hat VS White Hat



# Hacker



Hacker è un termine della lingua inglese che designa una persona che utilizza le proprie competenze informatiche per esplorare i dettagli dei sistemi programmabili e sperimenta come estenderne l'utilizzo. [Wikipedia](#)

Feedback

**Title** : Hacker's Manifesto

**Author** : The Mentor

==Phrack Inc.==

Volume One, Issue 7, Phile 3 of 10

=====

The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

Written on January 8, 1986

=====

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"....  
Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my world...

Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...

Damn underachiever. They're all alike.

you call us criminals. we explore... and you call us criminals. we seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals.

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Mentor+++

---

# Hacking E-zines

Museo delle e-zine italiane di  
Hacking  
Cracking  
Phreaking  
Virii  
Anarchy  
di qualche tempo fa.



- 
- Sono state omesse (quasi!) informazioni il cui scopo e' recare danno a persone.
  - Alcuni file posso essere considerati infetti da una scansione antivirus perche' contengono virus o trojan.
- 

## Butchered From Inside

L' e-zine del gruppo s0ftp�r0ject

## Dirty Net

numero 1	[ <a href="#">txt</a> ]	[ <a href="#">zip</a> ]
numero 2	[ <a href="#">txt</a> ]	[ <a href="#">zip</a> ]
numero 3	[ <a href="#">txt</a> ]	[ <a href="#">zip</a> ]
numero 4	[ <a href="#">txt</a> ]	[ <a href="#">zip</a> ]



DEF CON CTF 2021 ran Friday August 6<sup>th</sup> through Sunday 8<sup>th</sup> ([CTFTIME](#)) and were hybrid, like the rest of DEF CON.

**Finals** are over, congratulations Katzebin!

### Scoreboard (click on things!)



# Ecco i mHackeroni, lo special team italiano di cybersecurity che volerà al Defcon

di Flavio Fabbri | 7 Agosto 2019, ore 13:23



"Anche quest'anno saremo tra i finalisti: abbiamo infatti confermato gli ottimi risultati ottenuti



# Ecosystem

# Type of actors



Organised Crime



Angry People



Hacktivists



Competitors

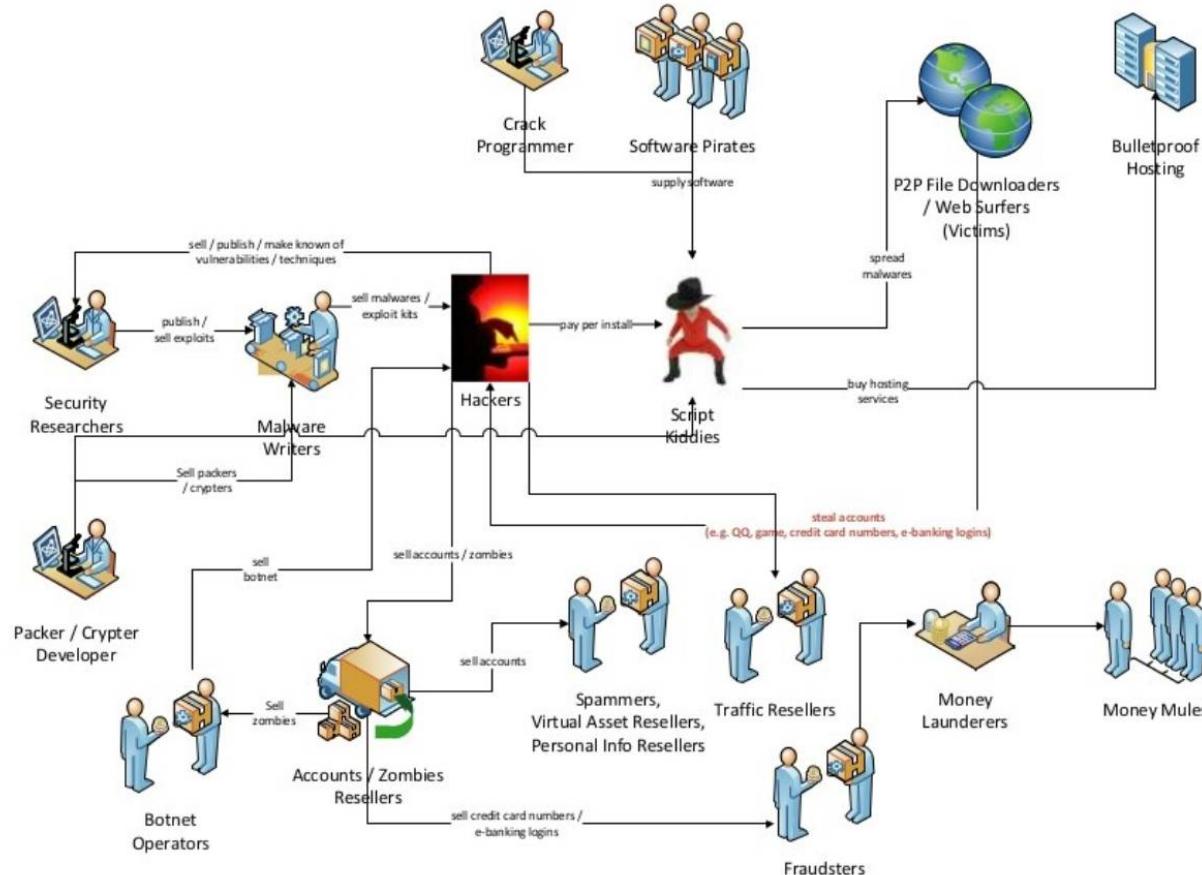


Script Kiddies



Nation States

# CYBERCRIME ECOSYSTEM





# Money Muling

Stay Safe with CIMB Clicks



Fraudsters contact potential victims via emails, chat rooms, job websites or blogs, and persuade them to receive money into their bank accounts, in exchange of attractive commissions.



The fraudsters then transfer the illegal money into the money mule's account.



When such frauds are reported, the money mule becomes the target of police investigations.



The money mule is then instructed to transfer the money to another money mule's account.

# Deep Web: Mixers / Tumbler



darknerk

My Purchases

 Search

## Categories

0-Day exploits (5)

- FUD Exploits (5)
- 1Day Private Exploits (5)

Information (37)

- Money (49)
- Source Code (12)
- Spam (3)
- Accounts (54)
- Cards (9)
- Tutorials (120)

Other Tools (14)

- RATs (4)
- Hardware (3)

Drugs (4)

- Misc (25)

## Category: 1Day Private Exploits

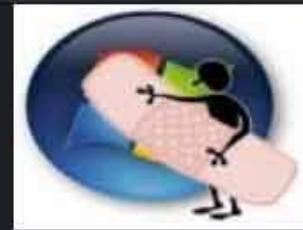
No Image

Anti-VPN and Proxy

\$ 1,572.51 - bestbuy



0 reviews



cve 2015-0057 Windows LPE

\$ 2,728.44 - ExploitFun



0 reviews



\*NEW\* ring0 LPE Exploit CVE-1

\$ 10,952.41 - PlayBit



0 reviews

No Image

MS15-034 Microsoft IIS Remote

\$ 74,881.44 - bestbuy



0 reviews



Netis / Netcore router RCE

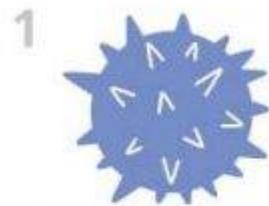
\$ 1,023.17 - bestbuy



0 reviews

# Attacks

# TOP 15 CYBER THREATS



Malware



Web-based attacks



Phishing



Web application attacks



Spam



DDoS



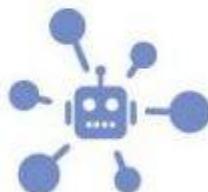
Identify theft



Data breach



Insider threat



Botnets



Physical manipulation,  
damage, theft and loss



Information leakage



Ransomware



Cyberespionage



Cryptojacking

# ALL YOUR FILES HAVE BEEN LOCKED!

This operating system and all of important data was locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

## Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! This computer is aimed to stop your illegal activity.

To unlock your files you have to pay the penalty!

You have only **96 hours** to pay the penalty, otherwise you will be **arrested**!

You must pay the penalty through **Bitcoin Wallet**.

To pay the penalty and unlock your data, you should send the following code:



to our agent e-mails:

[thematrixhasyou9643@yahoo.com](mailto:thematrixhasyou9643@yahoo.com) or

[cremreihanob1979@yandex.ru](mailto:cremreihanob1979@yandex.ru)

You will receive all necessary instructions!



# HURRY UP OR YOU WILL BE ARRESTED!!!

# Ransomware Gangs Leaks Sensitive Data Allegedly Stolen from Two More Healthcare Providers

Home

HIPAA Breach News

Ransomware Gangs Leaks Sensitive Data Allegedly Stolen from Two More Healthcare Providers

Posted By HIPAA Journal on Feb 17, 2021

100010101010001110110000001  
001001101111001101011111010  
1011111001010101001011001  
000101 **Ransomware** 100100  
11011101111011110100010  
111100010101001011001  
011011010001111010110

Share this article on:

 Facebook

 Twitter

 LinkedIn

The Conti ransomware gang has published data on its leak site which was allegedly obtained in an attack on Rehoboth McKinley Christian Health Care Services in New Mexico. The leaked data includes sensitive patient information including scanned patient ID cards, passports, driver's license numbers, diagnoses, treatment information, and diagnostic reports, although we have not been able to confirm the source of the

Search

Search

## HIPAA Compliance Checklist

Simple Guidelines  
Immediate PDF Download

Name \*

Work Email \*

Phone \*

Download FREE Checklist Now

Immediate Access  
[Privacy Policy](#)

L'ANALISI

# Regione Lazio e ransomware, lieto fine amaro: troppi errori fatti

Home > Malware e attacchi hacker

Condividi questo articolo



Un attacco ransomware non ha nulla di sofisticato, e dovrebbe ben rientrare nelle capacità di gestione di un'infrastruttura critica come la Regione Lazio, che dovrebbe aver adottato un piano di risposta agli incidenti di questo tipo, e per il ripristino delle operatività nel più breve tempo possibile. Ma così non è stato, con molti errori, tecnici e di comunicazione

08 Ago 2021



Matteo Navacci

Data protection counsel, DPO, Co-Founder Privacy Network



# Stuxnet, il virus informatico più distruttivo della storia

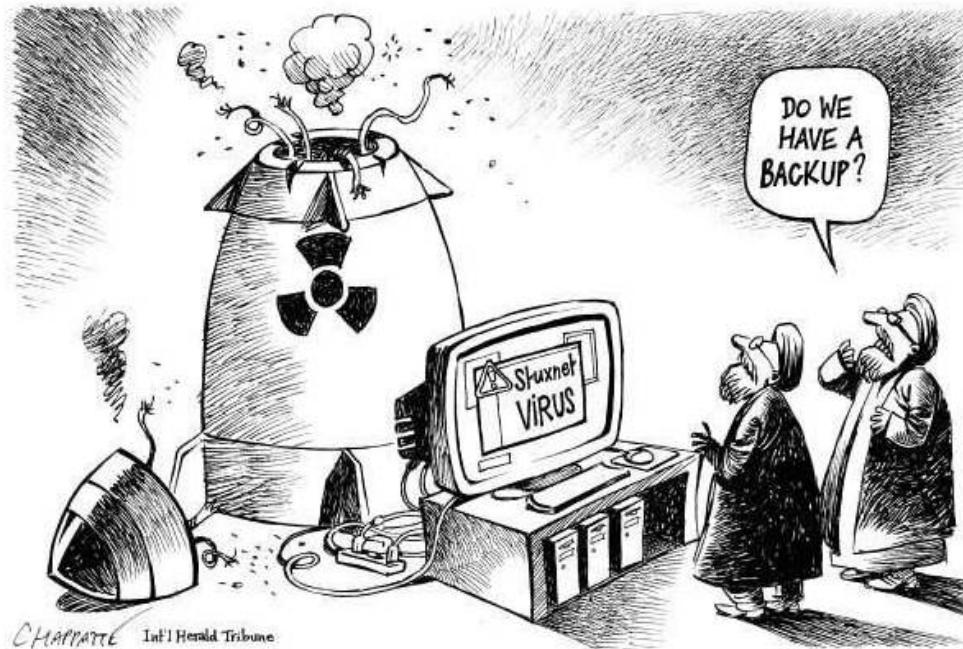
 Tweet

 Condividi

 Condividi

[ZEUS News - [www.zeusnews.it](http://www.zeusnews.it) - 13-07-2021]

Commenti (11)



Credits: Chappatte/International Herald Tribune

# 5 Best Free Spy Apps for Android (Updated 2019)

August 19, 2019 by Jack Gillman

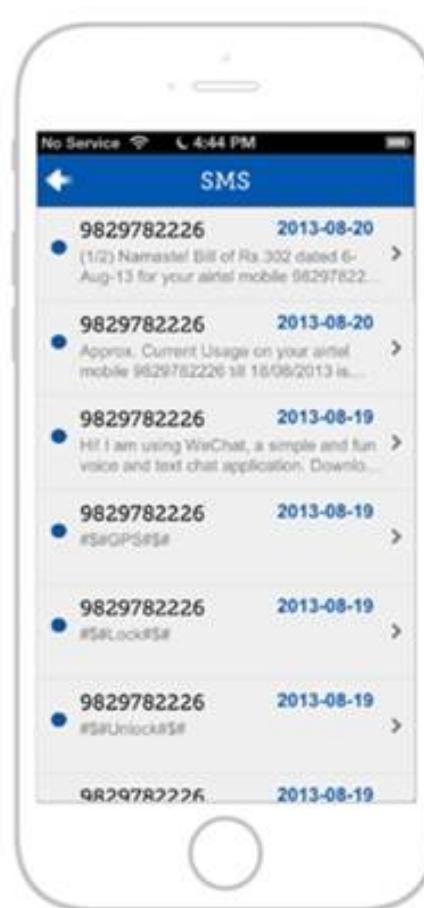
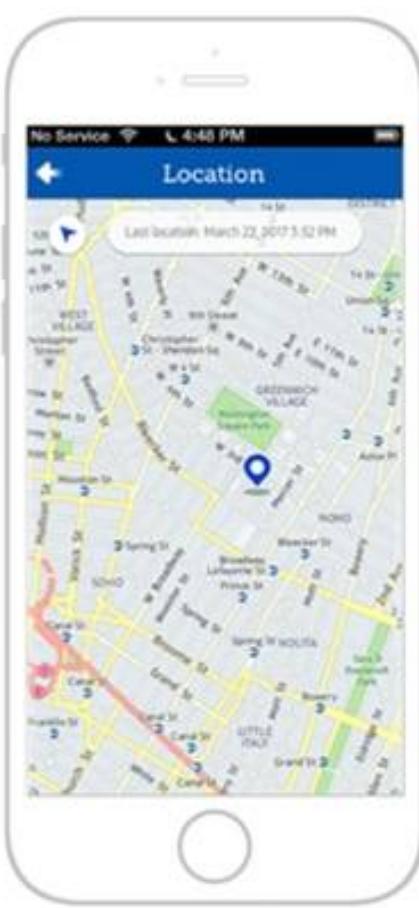
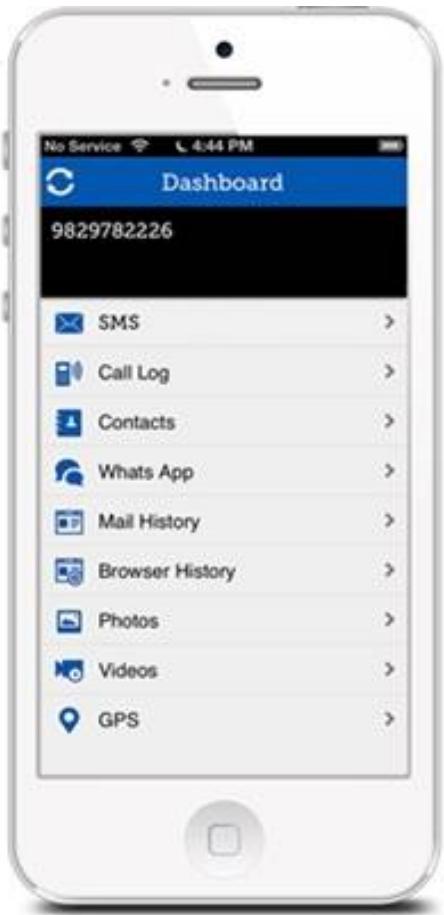


Are you looking for the best free Android spy apps? There are dozens of free spy apps for Android making it harder for beginners to choose from.

In this post, we have hand-picked five best **hidden spy apps** that you can download on your Android devices. Most of these apps allow you to monitor without needing to "Root" the device.

[How to Spy on an Android Phone](#)

---



# REMEMBER...



TO HAVE FUN!

@embyte