Guerre di rete.
Come Internet ha visto l’ascesa di conflitti digitali, hacking di Stato e cybercrimine

@carolafrediani - 100° Mercoledì di Nexa

Dichiarazione d'indipendenza del Cyberspazio

di John Perry Barlow

(English version)

Governi del Mondo, stanchi giganti di carne e di acciaio, io vengo dal Cyberspazio, la nuova dimora della Mente. A nome del futuro, chiedo a voi, esseri del passato, di lasciarci soli. Non siete graditi fra di noi. Non avete alcuna sovranit&#65533; sui luoghi dove ci incontriamo.

Noi non abbiamo alcun governo eletto, &#65533; anche probabile che non ne avremo alcuno, cos&#65533; mi rivolgo a voi con una autorit&#65533; non pi&#65533; grande di quella con cui la libert&#65533; stessa, di solito, parla. Io dichiaro che lo spazio sociale globale che stiamo costruendo &#65533; per sua natura indipendente dalla tirannia che voi volete imporci. Non avete alcun diritto morale di governarci e non siete in possesso di alcun metodo di costrizione che noi ragionevolmente possiamo temere.

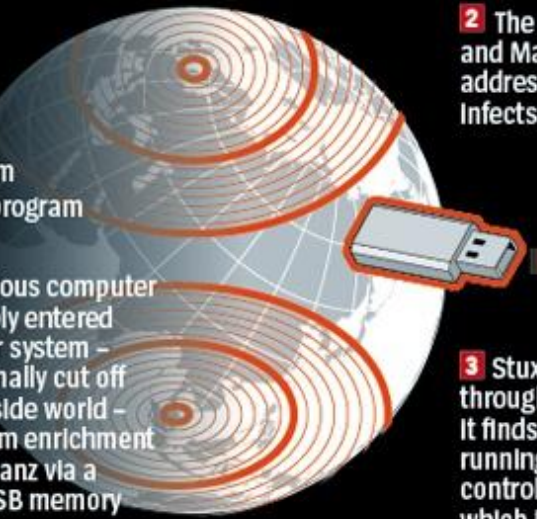
I Governi ottengono il loro potere dal consenso dei loro sudditi. Non ci avete chiesto n&#65533; avete ricevuto il nostro. Noi non vi abbiamo invitati. Voi non ci conoscete e non conoscete neppure il nostro mondo. Il Cyberspazio non si trova all'interno dei vostri confini.

Non pensate che esso si possa costruire come se fosse il progetto di un edifico pubblico. Non potete. &#65533; un atto di natura e si sviluppa per mezzo delle nostre azioni collettive. Non siete stati coinvolti nelle nostre grandi e partecipate discussioni e non avete creato il valore dei nostri mercati. Voi non conoscete la nostra cultura, la nostra etica, e nemmeno i codici non scritti che danno alla nostra societ&#65533; piu' ordine di quello che potrebbe essere ottenuto dalle vostre imposizioni.

Voi affermate che ci sono problemi fra di noi che hanno necessit&#65533; di essere risolti da voi. Voi usate questa affermazione come un pretesto per invadere le nostre aree. Molti di questi problemi non esistono. Troveremo i conflitti reali e le cose che non vanno e li affronteremo con i nostri mezzi. Stiamo costruendo il nostro Contratto Sociale.
Questo potere si svilupper&#65533; secondo le condizioni del nostro mondo, non del vostro. Il nostro mondo &#65533; differente.

Software Sabotage

How Stuxnet disrupted Iran's uranium enrichment program



1 The malicious computer worm probably entered the computer system – which is normally cut off from the outside world – at the uranium enrichment facility in Natanz via a removable USB memory stick.

2 The virus is controlled from servers in Denmark and Malaysia with the help of two Internet addresses, both registered to false names. The virus infects some 100,000 computers around the world.

3 Stuxnet spreads through the system until it finds computers running the Siemens control software Step 7, which is responsible for regulating the rotational speed of the centrifuges.

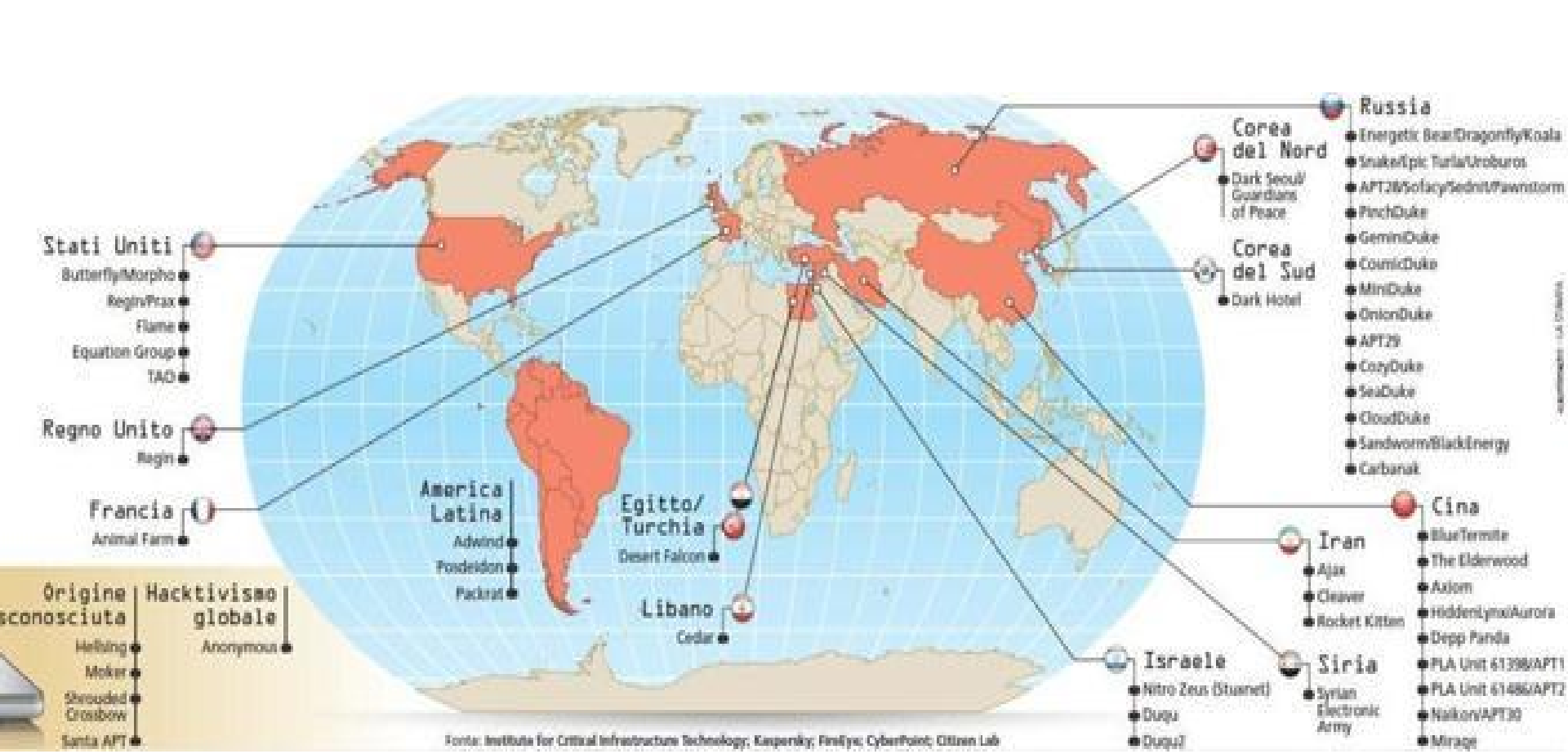
4 The computer worm varies the rotational speed of the centrifuges. This can destroy the centrifuges and impair uranium enrichment.

Iranian centrifuges for uranium enrichment

DER SPIEGEL

5 The Stuxnet attacks start in June 2009. From this point on, the number of inoperative centrifuges increases sharply.

Source: IAEA, ISIS, FAS, World Nuclear Association, FT research


Stati Uniti
Butterfly/Morpho
Regin/Prax
Flame
Equation Group
TAO
Regno Unito
Regin
Francia
Animal Farm
America Latina
Adwind
Poseidon
Packrat
Egitto/ Turchia
Desert Falcon
Libano
Cedar
Israele
Nitro Zeus (Stuxnet)
Duqu
Duqu2
Siria
Syrian Electronic Army
Iran
Ajax
Cleaver
Rocket Kitten
Cina
BlueTermite
The Elderwood
Axiom
HiddenLynx/Aurora
Deep Panda
PLA Unit 61398/APT1
PLA Unit 61486/APT2
Naikon/APT30
Mirage
Corea del Nord
Dark Seoul/ Guardians of Peace
Corea del Sud
Dark Hotel
Russia
Energetic Bear/Dragonfly/Koala
Snake/Epic Turla/Uroburos
APT28/Sofacy/Sednit/Pawnstorm
PinchDuke
GeminiDuke
CosmicDuke
MiniDuke
OnionDuke
APT29
CozyDuke
SeaDuke
CloudDuke
Sandworm/BlackEnergy
Carbanak
Origine sconosciuta
Hellsing
Moker
Shrouded Crossbow
Santa APT
Hacktivismo globale
Anonymous
Fonte: Institute for Critical Infrastructure Technology; Kaspersky; FireEye; CyberPoint; Citizen Lab

Cyberspace is an active battleground, with cybercriminals, government agents and even military personnel probing weaknesses in corporate, national and even personal online defense - **Dorothy Denning,** ***Emeritus Distinguished Professor of Defense Analysis, Naval Postgraduate School***

RECKLESS EXPLOIT

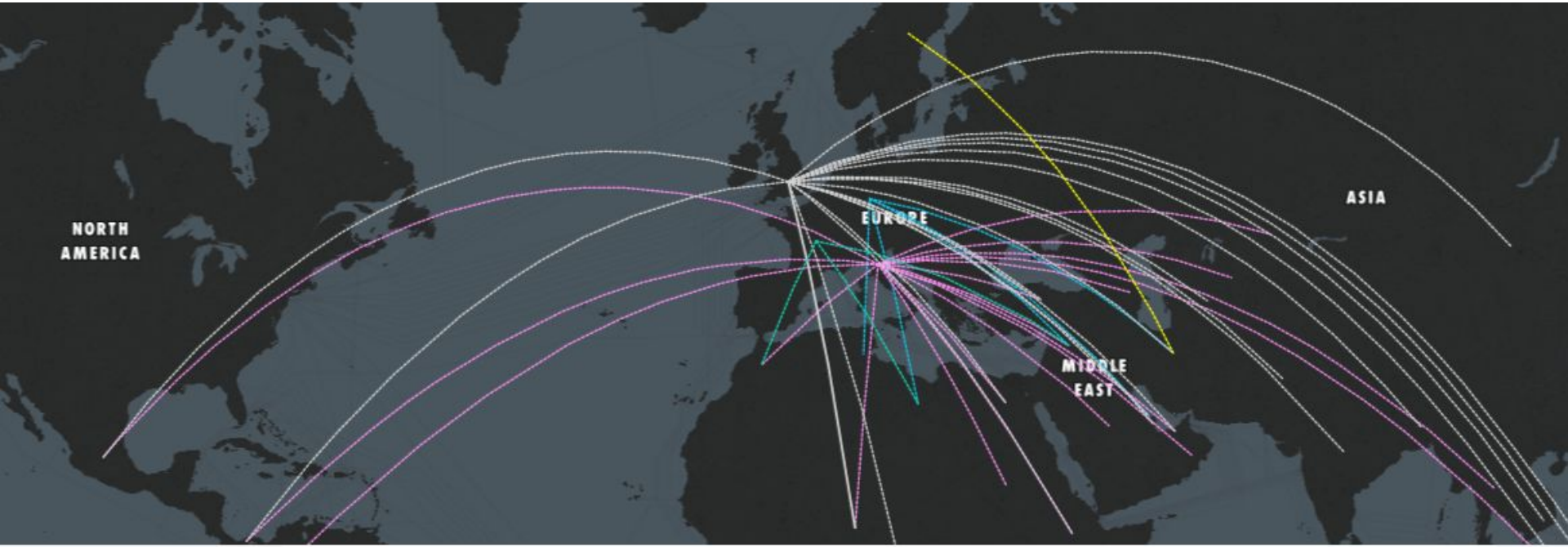
Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware

By John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert

June 19, 2017 Lea la investigación de R3D, SocialTic y Articulo19 (in Spanish)

This report is Part 3 of a series on the abuse of NSO Group's spyware.

Part 1: The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender
Part 2: Bittersweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links
Part 3: Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware
Part 4: Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware
Part 5: Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware
Part 6: Reckless IV: Lawyers For Murdered Mexican Women's Families Targeted with NSO Spyware
Part 7: Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware

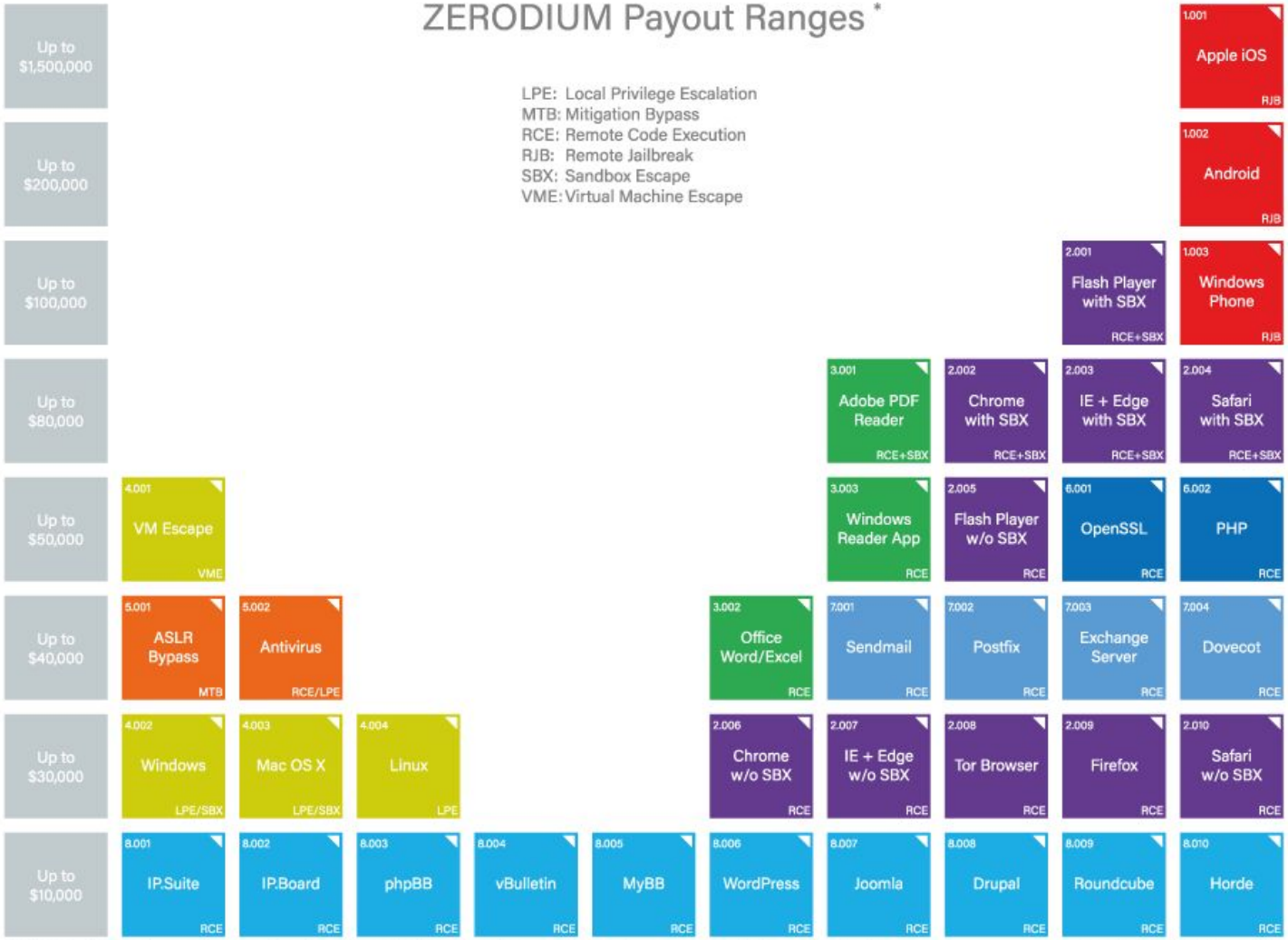


HOW EUROPE EQUIPS THE WORLD WITH SURVEILLANCE TECHNOLOGY AND WHAT WE WANT TO CHANGE ABOUT IT

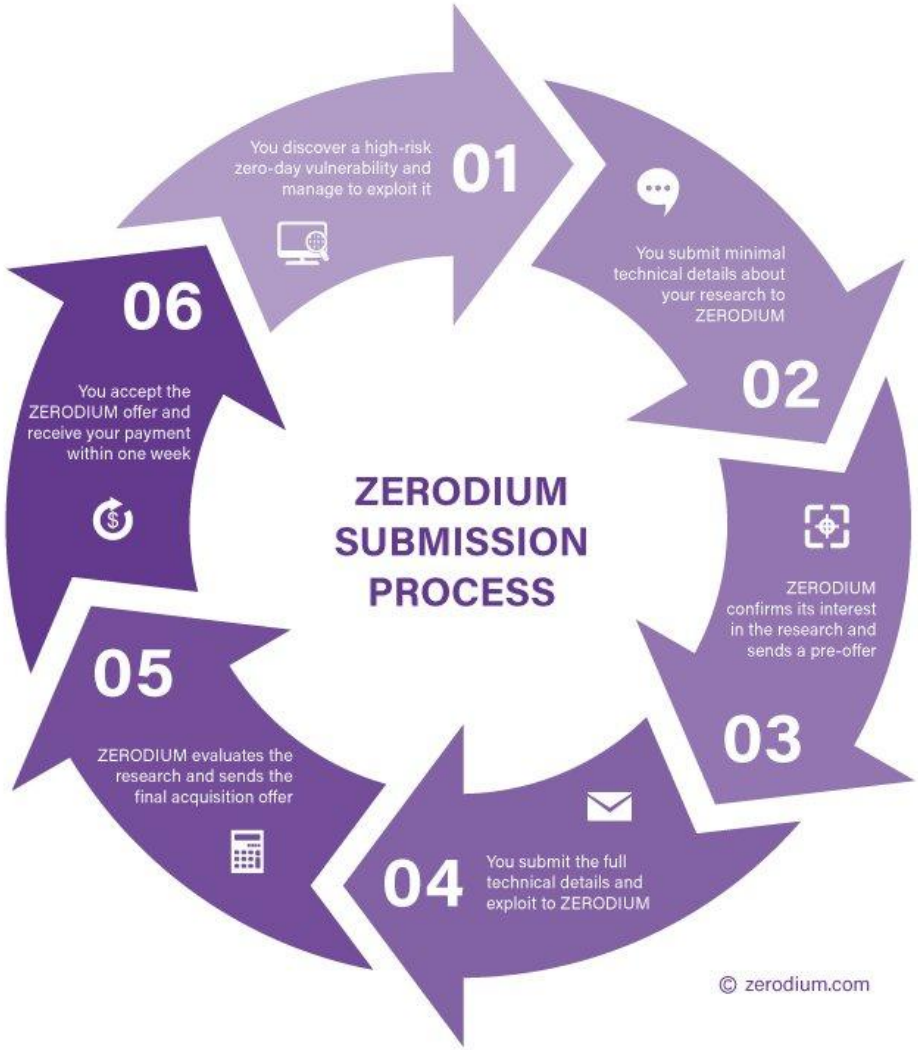

Name
Size
BANANAGLEE
6 items
BARGLEE
1 item
BLATSTING
7 items
BUZZDIRECTION
2 items
EXPLOITS
8 items
OPS
6 items
SCRIPTS
33 items
TOOLS
15 items
TURBO
2 items
NSA HACKED!
Private Hacking Tools & Exploits Leaked
NATIONAL SECURITY AGENCY

ZERODIUM Payout Ranges *

LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape



** All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.*


ZERODIUM SUBMISSION PROCESS
01
You discover a high-risk zero-day vulnerability and manage to exploit it
02
You submit minimal technical details about your research to ZERODIUM
03
ZERODIUM confirms its interest in the research and sends a pre-offer
04
You submit the full technical details and exploit to ZERODIUM
05
ZERODIUM evaluates the research and sends the final acquisition offer
06
You accept the ZERODIUM offer and receive your payment within one week
© zerodium.com

Le piratage de TV5 Monde revendiqué par un groupe djihadiste

Des documents présentés comme des pièces d'identité et des CV de proches de militaires français impliqués dans les opérations contre l'Etat islamique ont été publiés sur le compte Facebook de TV5 Monde.

Le Monde.fr avec AFP | 09.04.2015 à 00h22 • Mis à jour le 09.06.2015 à 19h03

Les chaînes, le site Web et plusieurs pages Twitter et Facebook du groupe télévisé francais TV5 Monde ont été victimes mercredi 8 avril vers 22 heures d'une

- June, 2016 - DNC Hack
- June, 2016 - Crowdstrike: attribution to Russia (FSB and GRU)
- June, 2016 - “Romanian” Guccifer 2.0 claims the hack
- July 22, 2016 - Wikileaks publishes DNC emails
- July, 2016 - The FBI announces an investigation
- September, 2016 - Trump: it could have been anyone
- October-November 2016 - Wikileaks releases John Podesta’s emails
- October, 2016 - DCLeaks publishes other Democratic documents
- October 7, 2016 - US gov officially blames Russia
- December 29, 2016 - President Obama issues an executive order with sanctions against Russia
- January 2017: report by US intelligence accusing Putin to have ordered cyberattacks against the Democrats
- January 2017: news about Russia arresting (in December) security researcher Ruslan Stoyanov, and two FSB official: Sergei Mikhailov and Dmitry Dokuchaev
- February 13, 2017 - Trump’s national security adviser Michael Flynn resigns over his phone calls with Russian ambassador
- March 2017: US charges against 4 men, including two US spies (from FSB, including Dokuchaev), for the Yahoo hack in 2014
- March 2017 - FBI director James Comey confirms that the FBI is investigating links between Russia and members of the Trump campaign

OPINION

False Flags: The Kremlin's Hidden Cyber Hand

The Islamic State's hacking army doesn't actually work for ISIS—It's part of the secret Russian online espionage effort against the West

By John R. Schindler • 06/18/16 12:15pm

We've adopted the following terminology to refer to these concepts:

Information (or Influence) Operations - Actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts (false amplifiers) aimed at manipulating public opinion.

False News - News articles that purport to be factual, but which contain intentional misstatements of fact with the intention to arouse passions, attract viewership, or deceive.

False Amplifiers - Coordinated activity by inauthentic accounts with the intent of manipulating political discussion (e.g., by discouraging specific parties from participating in discussion, or amplifying sensationalistic voices over others).

Disinformation - Inaccurate or manipulated information/content that is spread intentionally. This can include false news, or it can involve more subtle methods, such as false flag operations, feeding inaccurate quotes or stories to innocent intermediaries, or knowingly amplifying biased or misleading information. Disinformation is distinct from **misinformation**, which is the inadvertent or unintentional spread of inaccurate information without malicious intent.

ŦΞCHIПĐUSŢRY @techindustry · 1h
@RealJohnnyZ

@FBI THIS IS AN ACTIVE MEASURE ACCOUNT.

Thanks for doing such a great job!

2

JohnnyZ @RealJohnnyZ · 48m
#Choose wisely #France #Macronhacks #MacronLeaks #MacronNonMerci #MacronGate #BayrouGate #Marine2017 #JeVotePour🇫🇷 #avoté🇫🇷 #LePenOui

2 4 2

Twitta una risposta

Tweet

🐸 Pepe 🍗 Hanson 🇦🇺
@pepe_hanson

OwO
got it bad, got it bad, got it bad,
I'm hot for teacher
I got it bad, so bad,
I'm hot for teacher 🎶 🎶 🎶
#MacronGate #MacronLeaks

Lingua originale: inglese; traduci