



ODAID

Organización de Ayuda Integral para el Desarrollo



Ciberseguridad para Organizaciones Sin Fines de Lucro



Eduardo Snape (Prof. Snape)



- ❑ Entusiasta de la tecnología, comunidades y el aprendizaje colaborativo.
- ❑ 26 años de experiencia profesional
- ❑ Director de Tecnología para un despacho legal
- ❑ Director de la Fundación Comunidad DOJO
- ❑ Instructor técnico y docente universitario
- ❑ Miembro del equipo organizador de las comunidades BSides Panamá, Hackthebox Panamá, Owasp Panamá, Azure User Group y Asesor de WOSSEC Panamá

Contactos

- ❑ Web: www.comunidadojo.org
- ❑ Correo: Info@comunidadojo.org
- ❑ youtube: <https://www.youtube.com/fundacioncomunidadojo>
- ❑ twitter: [@comunidadojo](https://twitter.com/comunidadojo)



Sheila I. Pérez de Ávila

- Ingeniera en Sistemas Telemáticos
- Magister en Gerencia de Sistemas y Seguridad Informática
- +15 años de experiencia en Tecnología



Embajador - Fundación Comunidad Dojo



Women of Security – Chapter Panamá

Agenda

- ¿Son las OSFL interesantes para un cibercriminal?
- ¿Quiénes nos pueden atacar?
- ¿Cómo nos atacan?. Técnicas y tácticas
- Medidas sencillas de protección
- Control parental y Teletrabajo

¿Cuál es la ODS con el que más se conecta su OSFL?



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

slido

Su OSFL o alguna que conozca ha sido víctima de un ciberataque?

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

CASOS LOCALES



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

¿Son las OSFL interesantes para un cibercriminal?

0%

0%

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

OSFL: ¿Somos un objetivo para los cibercriminales?

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

¿Por qué? ¿Qué tiene una OSFL que interese a un cibercriminal?

Datos de donantes,
voluntarios, colaboradores
(personales, médicos)

Dinero
\$\$\$

Atacar a sus
directivos

Erradicar la
causa

Daño
Reputacional

Para afectar
operaciones
(Grants)

Para llegar a
otros

Por ser vulnerable



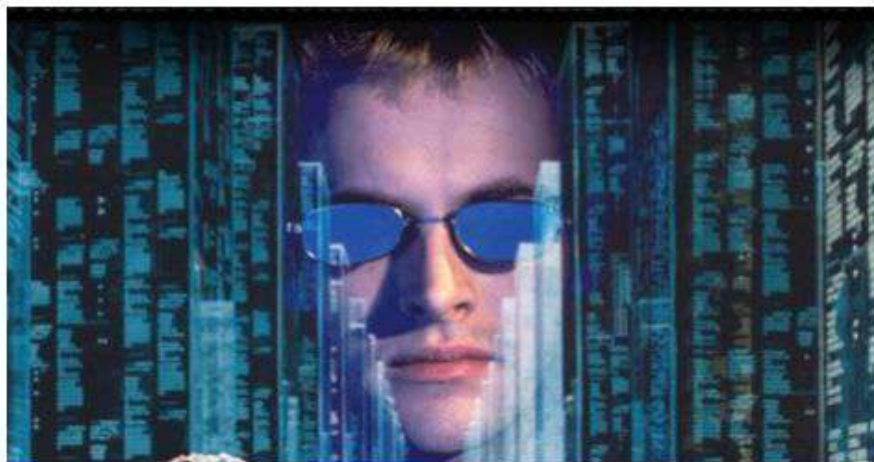
Russian hacking team The Dukes targeting NGOs and think tanks after Trump victory

John Biggs @johnbiggs / 5:55 AM EST • November 14, 2016

Comment



@comunidaddojo



According to Internet security team [Volexity](#) has detected an active spear-phishing effort by Russian hacker groups including Cozy Bear and the Dukes. The targeted phishing emails feature subject lines like "The "Shocking" Truth About Election Rigging" and a false "FYI" from the Clinton Foundation.

You can read about the efforts [on Volexity's own site](#) and [KrebsOnSecurity](#).

"Volexity observed five different attack waves with a heavy focus on U.S.-based think tanks and non-governmental organizations (NGOs)," the company wrote. "These e-mails came from a mix of attacker created Google Gmail accounts and what appears to be compromised e-mail accounts at Harvard's Faculty of Arts and Sciences (FAS). These e-mails were sent in large quantities to different individuals across many organizations and individuals focusing in national security, defense, international affairs, public policy, and European and Asian studies. Two of the attacks purported to be messages forwarded on from the Clinton Foundation giving insight and perhaps a postmortem analysis into the elections."

Noticias de ataques a OSFN





@comunidaddojo



Chinese Cyber-Espionage Group Targeted NGOs for Years

By Ionut Arghire on January 08, 2020



Share



Tweet



Recommend 0



RSS

A cyber-espionage group supposedly linked to the Chinese government is targeting non-governmental organizations (NGOs) in South and East Asia, Secureworks has revealed.

Referred to as BRONZE PRESIDENT, the group may have been active since at least 2014, also targeting political and law enforcement organizations and using both proprietary and publicly available tools to monitor the activity of targeted organizations, discredit their work, or steal their intellectual property.

The hackers use custom batch scripts to collect either specific file types or all files from a targeted NGO's systems, as well as credentials from high-privilege network accounts and sensitive accounts, including social media and webmail.

Evidence suggests the group has been targeting political and law enforcement organizations in countries such as Mongolia and India. The hackers appear interested in national security, humanitarian, and law enforcement organizations in East, South, and Southeast Asia, Secureworks says.

BRONZE PRESIDENT targets NGOs that conduct research on issues relevant to China, the group's infrastructure is linked to entities in China, a subset of the group's operational infrastructure is linked to China-based Internet service providers, and the hackers leverage tools such as PlugX, which have historically been used by Chinese threat groups.

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

COVID-19 brings wave of cyberattacks against NGOs

By **Rebecca Root** // 13 April 2020



Innovation & ICT Global Health CRS IFRC Mercy Corps

Our COVID-19 coverage is free. Please consider a Devex Pro subscription to support our journalism.



Photo by: Taskin.Ashiq on Unsplash

BELFAST, Northern Ireland — Aid groups say they are coming under an increased number of cyberattacks as they try to work through the disruption of COVID-19.

NGO leaders said attackers are hoping to benefit from money intended for the pandemic response and capitalize on weaknesses caused by the disruption.

ADVERTISEMENT

Make a world of difference.

Earn your master's degree entirely online

Northwestern
GLOBAL HEALTH
School of Professional Studies

LEARN MORE >

RELATED JOBS

- Individual Consultant: Nutrition Information Systems Specialist (National)
Uganda
- District Health Information System Officer
Myanmar
- Capacity Building and Collaboration

WHO said it is experiencing double the normal amount of cyberattacks as scammers “take advantage of the COVID-19 emergency” by sending fraudulent email and WhatsApp messages in an attempt “to steal money or sensitive information.” It issued staffers advice on how to prevent security breaches, which included double-checking email addresses and links, verifying any suspicious communication with WHO directly, and not opening email attachments from the agency that were not requested.

While Catholic Relief Services hasn't seen an increase in attacks, Vice President and Chief Information Officer Karl Lowe said the organization has similarly issued updated advice for staff. He said that cybersecurity requires a three-pronged approach covering people, processes, and technology — and that people are typically the weakest link, especially when overwhelmed or distracted, as might currently be the case.

COVID-19 — a timeline of the coronavirus outbreak

Follow the latest developments on the new coronavirus that causes COVID-19.



@comunidaddojo

“Los atacantes se aprovechan del miedo, la confusión y el estrés que experimentan las personas durante la pandemia.”

-Michael Boeglin, CIO, Mercy Corps

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

El panorama mundial



Top Riesgos Globales por probabilidad



	1st	2nd	3rd	4th	5th	6th	7th
2021	Extreme weather	Climate action failure	Human environmental damage	Infectious diseases	Biodiversity loss	Digital power concentration	Digital inequality

	1st	2nd	3rd	4th	5th
2020	Extreme weather	Climate action failure	Natural disasters	Biodiversity loss	Human-made environmental disasters
2019	Extreme weather	Climate action failure	Natural disasters	Data fraud or theft	Cyberattacks
2018	Extreme weather	Natural disasters	Cyberattacks	Data fraud or theft	Climate action failure
2017	Extreme weather	Involuntary migration	Natural disasters	Terrorist attacks	Data fraud or theft
2016	Involuntary migration	Extreme weather	Climate action failure	Interstate conflict	Natural catastrophes
2015	Interstate conflict	Extreme weather	Failure of national governance	State collapse or crisis	Unemployment
2014	Income disparity	Extreme weather	Unemployment	Climate action failure	Cyberattacks
2013	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Water crises	Population ageing
2012	Income disparity	Fiscal imbalances	Greenhouse gas emissions	Cyberattacks	Water crises





@comunidaddojo



Top Risks by likelihood

by likelihood

- 1 Extreme weather
- 2 Climate action failure
- 3 Human environmental damage
- 4 Infectious diseases
- 5 Biodiversity loss
- 6 Digital power concentration
- 7 Digital inequality
- 8 Interstate relations fracture
- 9 Cybersecurity failure
- 10 Livelihood crises

Top Risks by impact

by impact

- 1 Infectious diseases
- 2 Climate action failure
- 3 Weapons of mass destruction
- 4 Biodiversity loss
- 5 Natural resource crises
- 6 Human environmental damage
- 7 Livelihood crises
- 8 Extreme weather
- 9 Debt crises
- 10 IT infrastructure breakdown

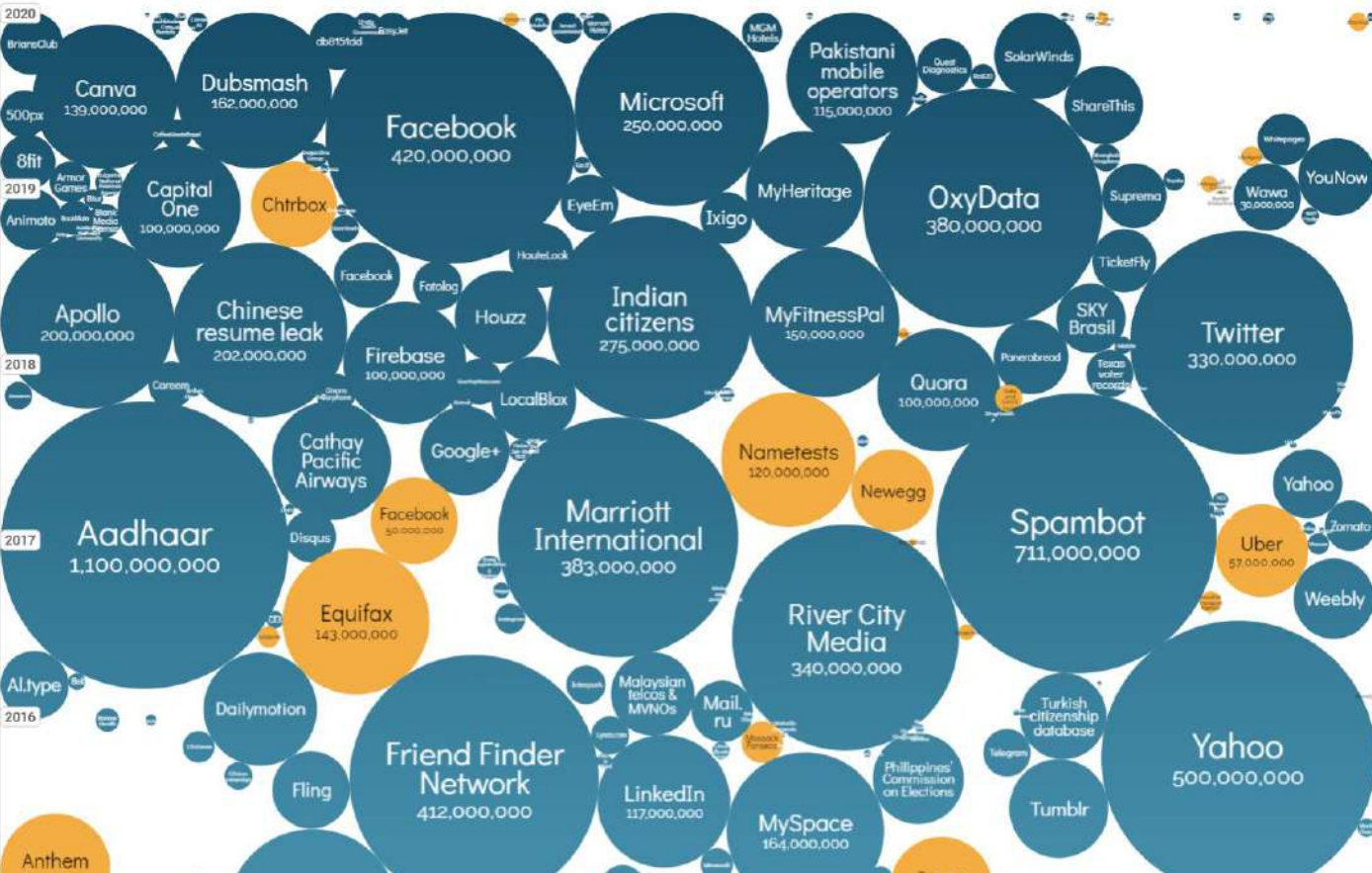
World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED Jan 2021

size: records lost filter

search...



@comunidaddojo

COMUNIDAD



DOJO

SEGURIDAD DE DATOS

<https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



@comunidaddojo

slido

¿Utiliza MFA?

MFA es un método de autenticación electrónica que debemos ingresar además de la contraseña para obtener acceso a un sitio web o aplicación.
Por ejemplo: un código, la huella digital, un token.





@comunidaddojo

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

pwned?



Generate secure, unique passwords for every account

[Learn more at 1Password.com](#)

[Why 1Password?](#)

359

pwned websites

7,840,611,051

pwned accounts

92,918

pastes

113,365,224

paste accounts

<https://haveibeenpwned.com/>

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Estadística de ataques por contraseñas

Stolen or Weak Passwords



Social Attacks
Social attacks, such as phishing, accounted for

Credential-Stealing Software



of breaches leveraged either stolen and/or weak passwords.



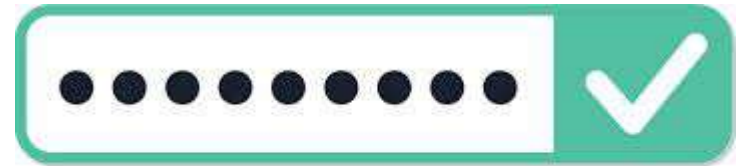
of attacks that resulted in a data breach.



of data breaches involved some form of credential-stealing malware.

La contraseña no es suficiente

- Al menos 65% de las personas utilizan la misma contraseña en varios sitios.
- Un 13% utiliza la misma contraseña en sus cuentas de redes y dispositivos.
- El 80% de las brechas de seguridad son causadas por password comprometidos.
- Las contraseñas comprometidas son responsables del 81% de los ataques de hacking.
- Un 49% de los colaboradores añade solo un dígito o cambian un caracter cuando requieren cambio de contraseña.





@comunidaddojo

The Most Popular Passwords Around the World

Most popular passwords appearing in leaks 2019/2020

	2020	change from previous year	2019
1.	123456*	0	123456*
2.	picture1	new	test1
3.	password	0	password
4.	111111	+7	zinch
5.	123123	+7	g_czechout
6.	senha**	new	asdf
7.	qwerty	0	qwerty
8.	abc123*	+65	iloveyou



* or variation ** Portuguese for password

Source: North Pass



statista

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

✓ Nice password!

- Your password is hack-resistant.
- Your password does not appear in any databases of leaked passwords

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo



LastPass by LogMeIn

How secure is your password?

See if your password is strong enough to keep you safe. This tool runs locally. No data is sent data over the internet.

Enter a password...

This tool is for personal testing purposes only. Nothing you enter is sent or recorded anywhere.

<https://lastpass.com/howsecure.php>



@comunidaddojo

The screenshot shows the LastPass web interface in a browser window. The browser tab is titled "My LastPass Vault" and the address bar shows "LogMeIn, Inc [US] | https://lastpass.com/vault". The interface has a dark grey sidebar on the left with navigation options: Collapse, All Items, Passwords, Notes, Addresses, Payment Cards, Bank Accounts, Driver's Licenses, Passports, Wi-Fi Passwords, Security Challenge (92%), Sharing Center, Emergency Access, Account Settings, and More Options. The main content area has a red header with "LastPass" and a search bar. Below the header, it says "All Items" and "Favorites (11)". The items are displayed in a grid:

- amazon.com (name@example.com)
- amazon Instant video (name@example.com)
- Dropbox (name@example.com)
- EVERNOTE (name@example.com)
- facebook (name@example.com)
- Google (name@example.com)
- Home WIFI
- hulu (name@example.com)
- NETFLIX (name@example.com)
- slack (name@example.com)
- verizon (name@example.com)

On the right side of the grid, there are buttons: "Add New Folder", "Share Item", "Add Secure Note", and "Add Site". The user profile in the top right shows "name@example.com Premium User".

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

¿Quién(es) los pueden atacar?

10%

10%



@comunidaddojo

¿Quién(es) los pueden atacar?

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Motivación, técnicas y tácticas



@comunidaddojo

ACTORES

MOTIVACIÓN

Cibercriminales



\$\$\$

Hactivistas



Ideológicas

Insiders



Descontento

Ciber Terroristas



Violencia ideológica

Patrocinados por
Gobiernos



Geopolíticas

Script Kiddies



Alimentar su ego

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

¿Cómo los atacan?



30%

30%

Tipos de Ataques más comunes



Ransomware



Malware



Phishing



Denial of Services

La plaga del secuestro informático mediante 'ransomware'

Otras dos ciudades de Estados Unidos aceptan pagar un rescate tras un ataque que ha dejado inutilizados todos sus sistemas



Monto del pago: 526.914 euros

Riviera Beach y Lake City

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



Time Remaining 10 Days or 14377 Minutes

Unlock Fee 0.35733 BTC \ 150 USD

Files Locked

System Status **Locked**

Your Computers Files have been Encrypted and Locked!

Your files have been encrypted and are unuseable and inaccessible. Don't worry, they're safe, for now.

This is unfortunate although for a small fee all of your Files will be returned to their original location as if nothing ever happened. Simply pay the recovery fee stated on this form and follow the instructions. Once the payment has been received your Files will be returned to normal. Not paying the Unlock Fee to the supplied Bitcoin Address before the Timer runs out means loss of all Files permanently.

The only payment accepted is Bitcoin. If you don't know what Bitcoin is there are instructions on how to obtain Bitcoin and pay the Fee. Just press the "How it Works" Button below to learn how Bitcoin works.

This software checks the Bitcoin Network for the exact payment amount on the Bitcoin address provided. Once the amount is confirmed by clicking "Confirm Payment" your files will be returned to their original locations.

Removing this software causes permanent loss of your files!

This software is the only way to get your files back!

Payment Address:

Copy

Review Locked Files

How it Works

How to Pay Unlock Fee

Check Payment Status



@comunidaddojo

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Garmin pagó millones de dólares por obtener la clave de descifrado del ransomware WastedLocker



@comunidaddojo

Publicado el 5 agosto 2020 por Juan Ranchal



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

RANSOMWARE como servicio de Suscripción

Stampado

- **Threat actor:** The rainmaker and others
- **Characteristics:**
 - Has a worm-like spreading functionality.
 - Will re-encrypt already encrypted files (other ransoms)
 - Stampado encrypts files using AES (Advanced Encryption Standard) and a Symmetric key encryption algorithm (which uses same key for encryption and decryption) with key length of 256.
- **Price:** \$39
- **Market:** Alphabay market (currently down)
- **Exploit kit:** sundown-pirate and RIG
- **IOC's:**
 - %AppData%\scvhost.exe
 - %AppData%\<Hexdecimalname>
 - %AppData%\<Hexdecimalname>
 - [DrivePath]\myDisk\drivers.exe
 - <filepath>/<encryptedname>.locked
 - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" "Windows Update"
%AppData%\scvhost.exe

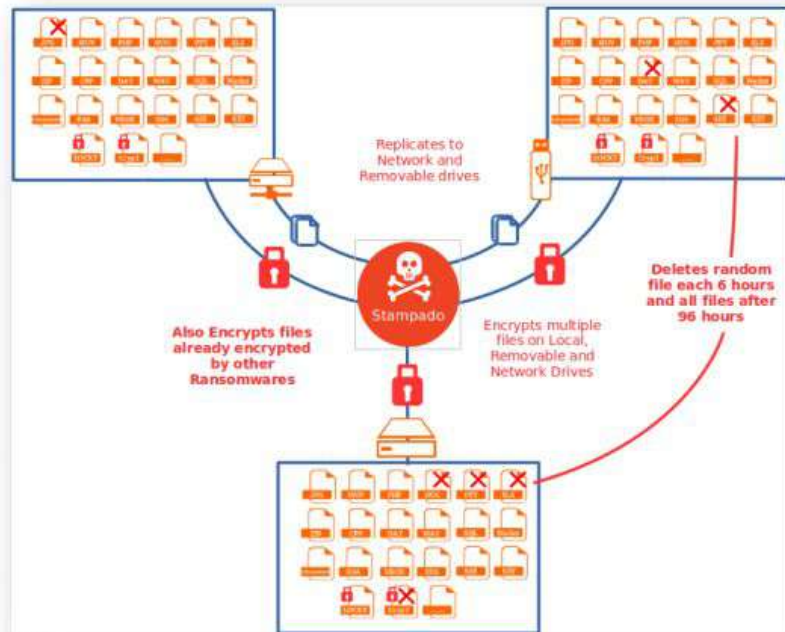


Figure 1: Stampado overall activity diagram

NHS Warns of New COVID-19 Vaccine-Related Phishing Campaigns

 by David Bisson on February 1, 2021

The United Kingdom's National Health Service (NHS) warned that scammers are in the process of sending out fake COVID-19 vaccine invitations. On January 25th, Urology Cancer Research & Education (UCARE) Oxford reached out to the NHS on Twitter and shared an image of one such fake invitation that it had received.

The Makeup of a Recent COVID-19 Scam Invitation

The scam email arrived with the subject line "NHSVaccination," and it used stolen branding in an attempt to trick the recipients into thinking that the email was legitimate. In its body, the attack message informed the recipient that the NHS was in the process of "performing selections for coronavirus vaccination on the basis of family genetics and medical history."

It then informed the recipient that they had been selected to receive the vaccine, at which point it instructed them to either accept or decline their invitation to receive the vaccine by clicking on one of two corresponding embedded links:

Phishing



@comunidaddojo

NHS

Test and Trace

This is a public health message from NHS

As part of the government's coordinated response to Coronavirus, NHS is performing selections for coronavirus vaccination on the basis of family genetics and medical history. .

You have been selected to receive a coronavirus vaccination.

Use this service to confirm/reject your coronavirus (COVID-19) vaccination:

[>> NHS - Accept invitation](#)

[>> NHS - Decline invitation](#)

A screenshot of the scam email (Source: Twitter)

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Banco de Chile, virus para distraer y luego robo por 10 Millones de dólares en la red SWIFT, 24 de Mayo

Banco de Chile #BancodeChile el 24 de Mayo sufrieron un virus que afectó a más de 9000 Pcs distraiendo al personal del Banco en su solución y en paralelo robaron aprox. US\$10 Millones en la red interna SWIFT. Es uno de los incidentes más grandes registrados en nuestra región. Recomiendo estudiar el caso y replicar medidas del Banco como activación de su plan de contingencia y ahora mejoras legales por parte del gobierno entre otras medidas de la superintendencia de Bancos #ciberseguridad

COMUNIDAD

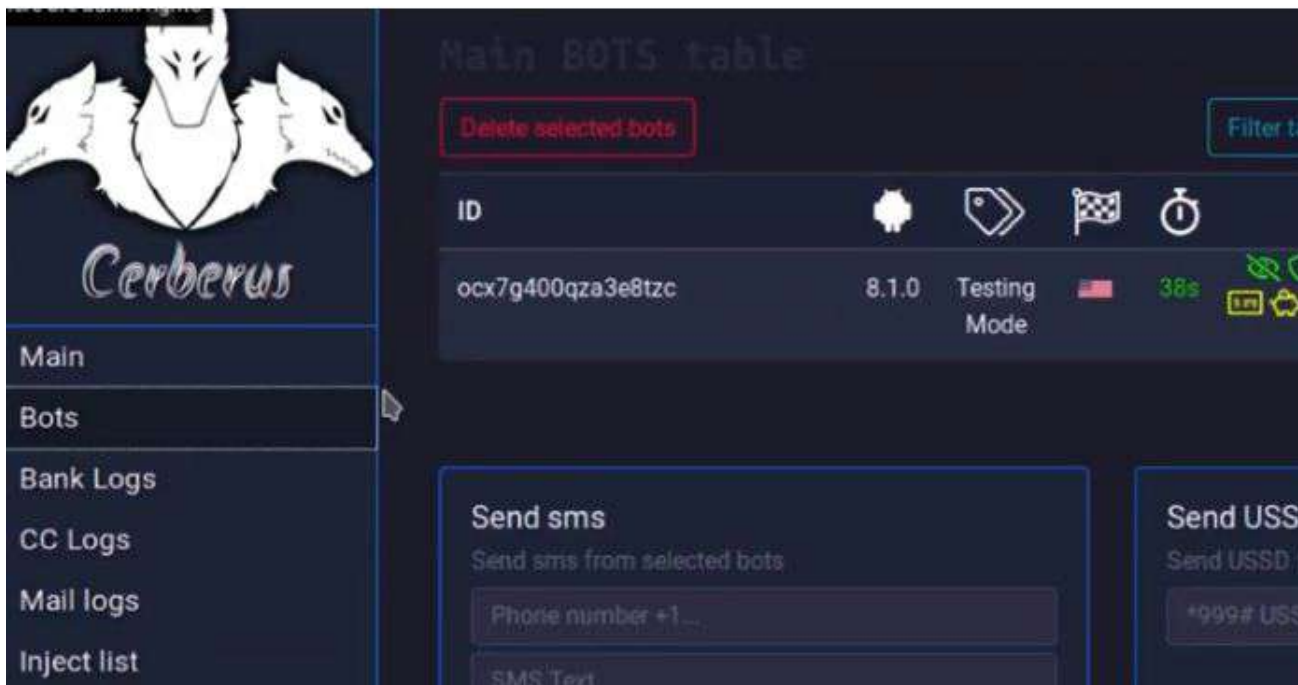


DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Cerberus: A New Android 'Banking Malware For Rent' Emerges

By — Swati Khandelwal · 13 Aug, 2019



Google stops biggest-ever distributed denial-of-service cyber attack

The cyber security threats such as distributed denial-of-service (DDoS) are growing exponentially, disrupting businesses of all sizes globally, leading to outages and loss of user trust

Topics

Google | Cyber Attack | Hacking

IANIS | New Delhi

Last Updated at October 17, 2020 10:57 IST



COMUNIDAD



DOJO

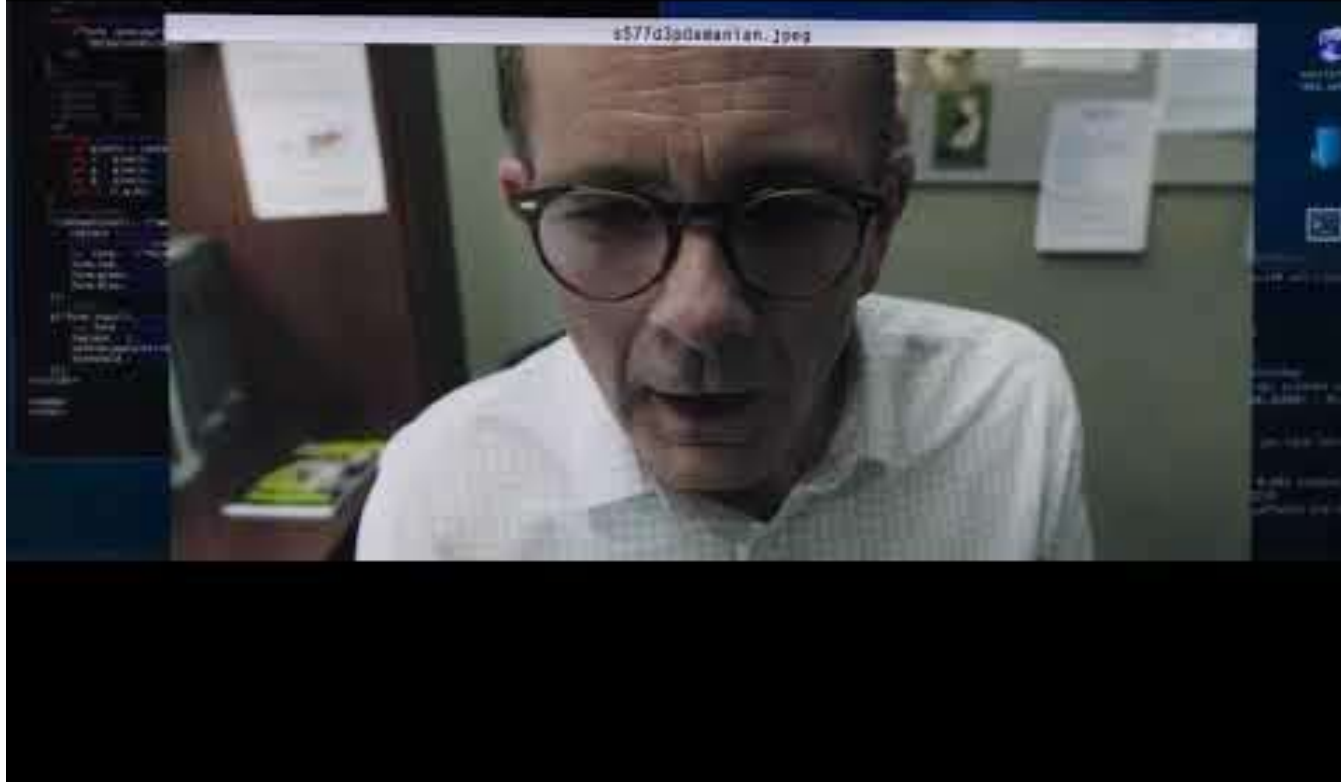
SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



Ataques dirigidos a personas



@comunidaddojo



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org · PANAMA

<https://www.youtube.com/watch?v=gJVHngzKMIs>



@comunidaddojo

INGENIERIA SOCIAL





Pensamiento, Rápido o lento

Daniel Kahneman.



@comunidaddojo

Sistema 1



Rápido



Inconsciente



Automático



Decisiones cotidianas



Propenso a errores

Sistema 2



Lento



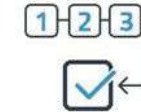
Consciente



Esforzado

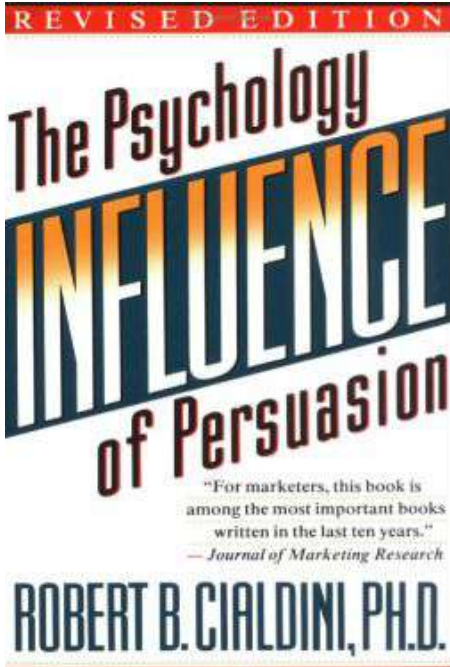


Decisiones complejas



Confiable

Cialdini's 6 Principles of Persuasion



Reciprocidad



Escasez



Autoridad



Consistencia



Simpatía



Consenso



@comunidaddojo

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org PANAMA



@comunidaddojo



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



Ataques Externos Indirectos (Ciberataques)



@comunidaddojo



Amazon's Alexa recorded private conversation and sent it to random contact



@comunidaddojo

The company, which has insisted its Echo devices aren't always recording, has confirmed the audio was sent





@comunidaddojo

¿Habrá
algo
PEOR...?

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



Ataques Externos – Cadena de Suministros (Proveedores)



@comunidaddojo



**BERMUDA CYBER ATTACK: WHY
SHOULD BILLIONAIRES BE WORRIED
ABOUT THE NEW APPLEBY DATA LEAK
AND SHOULD I BE AFRAID?**


The leak could be like the second round of the Panama Papers



**¿Habrá algo
PEOR...?**



SI.....LOS ATAQUES INTERNOS

A group of cheetahs is resting on a grassy field. One cheetah is lying down in the foreground, looking towards the camera. Another cheetah is lying down in the middle ground, looking away. A third cheetah is lying down in the background, looking away. The cheetahs have a distinctive spotted pattern on their fur. The grass is green and appears to be a mix of different species.

Insider

Un empleado, contratista o socio comercial actual o anterior que tenga o haya autorizado el acceso a la red, los sistemas o los datos de la organización.

Amenazas Internas

Intencionales

- Interrupción de servicios (IT Sabotaje)
- Fraude
- Espionaje (colocación de micrófonos) y cámaras)
- Extracción de información



Accidentales

- Fuga accidental de información, (Correos enviados por error).
- Pérdida de expedientes
- Pérdida de dispositivos electrónicos



@comunidaddojo

Medidas Sencillas de protección



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



@comunidaddojo

Estrategias de Mitigación

Recomendaciones sin costo o de muy bajo costo para apoyar el esquema de defensa contra las amenazas





@comunidaddojo

Controles Básicos - The Basics

- Educa a tus usuarios, principalmente a los directivos.
- Definir políticas y controles de seguridad simples y sostenible.
- No utilizar usuarios con permisos de administrador para el uso diario de su computador.
- Cambiar la configuración por defecto de equipos.
- Gestiona tus sistemas
 - Aplicar parches de seguridad
- Gestiona tus contraseñas
 - Utiliza contraseñas robustas
 - Cambia tus contraseñas con frecuencia
 - Considera utilizar un gestor de contraseñas
 - Incluye el doble factor de autenticación
- Prueba tus controles de seguridad



Realiza campañas de phishing



Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Settings

admin



Dashboard

Campaigns

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Settings

User Guide

API Documentation

Dashboard

Phishing Success Overview



Email Sent



Email Opened



Clicked Link



Submitted Data





¿Cómo minimizar los riesgos de amenazas internas?





1. Promover una cultura de valores compartidos, libre de humillaciones e injusticias



2. Educar






3. Poner atención a las conductas



4. Implementar controles básicos (the basics)

A group of seven business professionals, including men and women of various ethnicities, are standing in an elevator. They are dressed in professional attire like suits and blouses. The man on the far left is looking down at a mobile device. The woman in the center is holding a white briefcase. The woman on the far right is holding a white coffee cup. The elevator doors are open, and the background is a brightly lit hallway.

5. Promover una **cultura**
de Privacidad y protección de datos



Escritorios Limpios...no olvidar los
tableros

Impresión Segura



Triturar
documentos
sensitivos





Bloqueo automático y pantallas de Seguridad

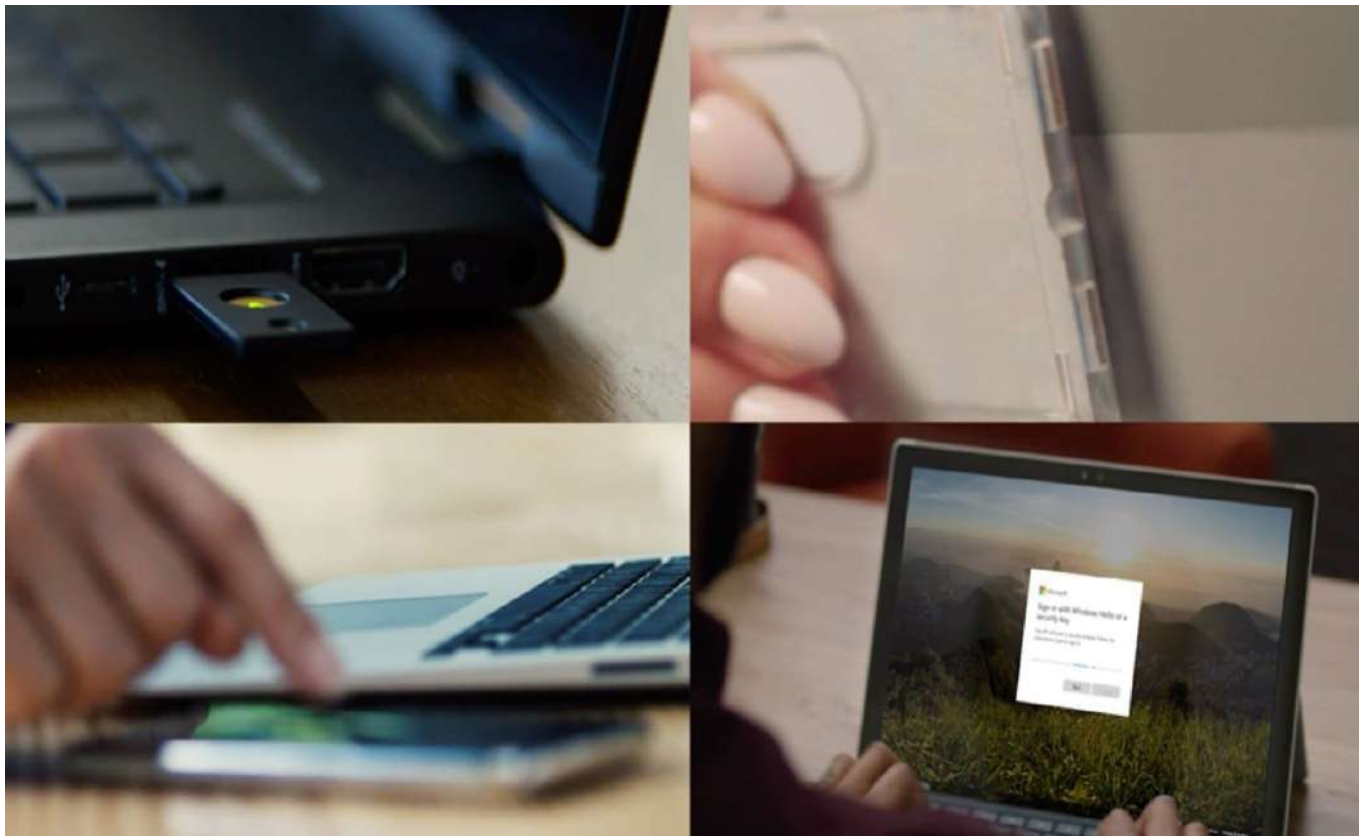


**Restringir y/o monitorear unidades
externas**

Menos Contraseñas (PasswordLess)



@comunidaddojo



COMUNIDAD



DOJO

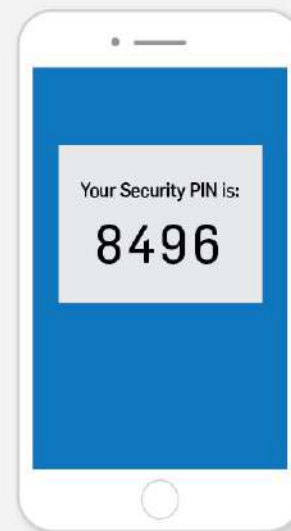
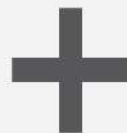
SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

2FA - MFA



@comunidaddojo

Two Factor Authentication



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



Seguridad en Casa



@comunidaddojo

Trabajo Remoto

Seguridad Personal

Control Parental





@comunidaddojo

Control Parental

Un alto % de menores navegan en Internet **sin** Filtrado de Contenido



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Características disponibles

- Control Web
- Control de aplicaciones
- Bloqueo de llamadas
- Tiempo de uso
- Geolocalización
- Botón de Emergencias

<https://securekids.es/caracteristicas/supervision-aplicaciones/>



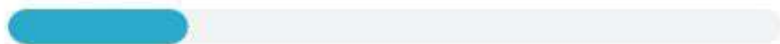
<https://www.gustodio.com>



@comunidaddojo

🕒 Media de uso diaria

4h 22m



Del Septiembre 4 al Septiembre 10



📊 Actividad principal

[Ver todo](#)





@comunidaddojo

Seguridad en Casa - Teletrabajo



Teletrabajo Seguro



- Cambiar contraseñas por defecto.
- Contraseñas Fuertes
- Actualizar el Sistema Operativo
- No usar “ Familias Solis wifi” como el nombre de su red.



BRINGING HI-TECH BACK TO LIFE



@comunidaddojo



COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



8 DojoTips para utilizar "Zoom" de forma segura:

- 1- Evite compartir el enlace a su reunión de forma pública.
- 2- No use una ID de reunión personal; use una ID de reunión única y una contraseña de reunión.
- 3- Deshabilite la opción "Unirse antes del host".
- 4- Deshabilite la opción "Permitir que los participantes eliminados vuelvan a unirse".
- 5- Habilite la sala de espera, ya que le permite aprobar a los asistentes antes de que se unan.
- 6- Establezca el uso compartido de pantalla en "solo host" (para evitar que terceros transmitan contenido molesto o inapropiado).
- 7- Deshabilite la transferencia de archivos (para evitar la transferencia de archivos maliciosos).
- 8- Una vez que todos los convocados y confirmados están presentes en la reunión, cierre su reunión.



zoom

Join a Meeting





@comunidaddojo

CONCLUSIONES



100%

100%

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA

Conclusiones

- Desarrollar una “**Cultura de Gestión de riesgo integral**” e incluir su monitoreo en la agenda de la junta directiva.
- Considere incluir un “**tech-savvy**” con miembro de la junta directiva o como parte de una junta asesora.
- **Capacitar, Capacitar**. Principalmente a los directivos.
- “**Do the basics**”. Principalmente si es un directivo.

Conclusiones

- Cambiar las contraseñas por defecto de los routers caseros
- Utilizar contraseñas robustas
- Actualizar sistemas operativos y aplicaciones
- Utilizar nombres adecuados en las redes WiFi



@comunidaddojo

IT'S QUIZ TIME

COMUNIDAD



DOJO

SEGURIDAD DE DATOS
OFENSIVA Y DEFENSIVA
www.comunidaddojo.org - PANAMA



FUNDACIÓN COMUNIDAD DOJO

Seguridad Defensiva y Ofensiva

MUCHAS GRACIAS POR SU ATENCION
Para consultas y oportunidades de colaboración
info@comunidaddojo.org
www.comunidaddojo.org

