



Impacto del COVID-19 en Organizaciones a Nivel Global

Manuela Jaramillo • Comercial para América Latina

manuela@intsights.com

Dark Web y Qué Podemos Conseguir?

FUGA DE CREDENCIALES

| | email | |
|---------|---------|--------------------------------------|
| | dan | whitepages.com: B22541 |
| | | whitepages.com: DEF637202C11 |
| stacy, | stacy, | sec |
| | | e.whitepages.com: DED913E5B7FD1DE41 |
| stacy, | stacy, | www |
| | | whitepages.com: 0645FE59D8C00A264 |
| tom, | tom | sec |
| | | e.whitepages.com: EDD913E5B A52F9621 |
| robert, | robert, | sec |
| | | e.whitepages.com: 2CD2BEAD C6368D281 |
| robert, | robert | www |
| | | whitepages.com: 6DAECE7 5802884 |
| sue, | | e.whitepages.com: BF 7A81620 |
| yanek, | | whitepa |

CUENTAS DE BANCO / BASES DE DATOS

...SH, UK, CA, AU, EU...other coun...

...ance 15000\$ = 800\$

Bank UK: (...)

Balance 5000 GBP = 200\$

Balance 10000 GBP = 500\$

Balance 16000 GBP = 700\$

Balance 20000 GBP = 1000\$

- + Bank To Bank Transfer To Any USA Bank
- + Bank To Bank Transfer To Any UK Bank
- + Bank To Bank Transfer To Any Euro Country Bank
- + Amount To Pay For That Depend On Amount You Want To Transfer
- + With Account Bank Login : Username + Password Number
- + I always check the balance and login details before selling

You can contact me for more and many Bank Logins you need.

...all details for login and I can transfer balance to your acc...

Bank Transfer To Any Usa Bank

Bank Transfer To Any Uk Bank

Bank Transfer To Any Euro Country Bank

...pend On Amount You Want

INFORMACIÓN PERSONAL

Collection 1 Breach - How To Find Out If Your Password Has Been Stolen

Kate O'Flaherty Contributor @Cybersecurity
I'm a freelance cyber security journalist.

Username
HACKER!!!

Password

ATAQUE DE NEGACIÓN DE SERVICIO – COMO SERVICIO



KITS O TUTORIALES DE PHISHING

gistrar IVA ID: 3370

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone:

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Name Server: EXPIRED1.NAMEBRIGHTDNS.COM

Name Server: EXPIRED2.NAMEBRIGHTDNS.COM

DNSSEC: unsigned

URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of whois database: 2019-03-25T10:12:13Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the registrar's sponsorship of the domain name registration in the registry is currently set to expire. This date does not necessarily reflect the expiration date of the domain name registrant's agreement with the sponsoring registrar. Users may consult the sponsoring registrar's Whois database to view the registrar's reported date of expiration for this registration.

OF USE: You are not authorized to access or query our Whois database through the use of electronic processes that are high-volume and except as reasonably necessary to register domain names or to maintain the database, you may not use the data for any other purpose, including, but not limited to, advertising, sales, promotion, or other commercial purposes. VeriSign Global Registry Services, Inc. ("VeriSign") is the registrar for this domain name registration record. VeriSign does not warrant the accuracy of the information in the Whois database. By using the Whois database, you agree to accept the terms and conditions of use.

Tácticas, Herramientas y Procedimientos

-Registro de Dominios y Phishing

- Aumento notorio de registro de dominios en el mes de marzo utilizando palabras como corona o covid.
- Finalizando 2019 , solo 190 dominios que hacían uso de estas palabras estaban registrados. Hoy, el numero sobrepasa los 35.000 registros.
- Correos de phishing organizaciones de salud o de gobierno para redirigir a las victimas a descargar malware que resulta en robo de información del dispositivo

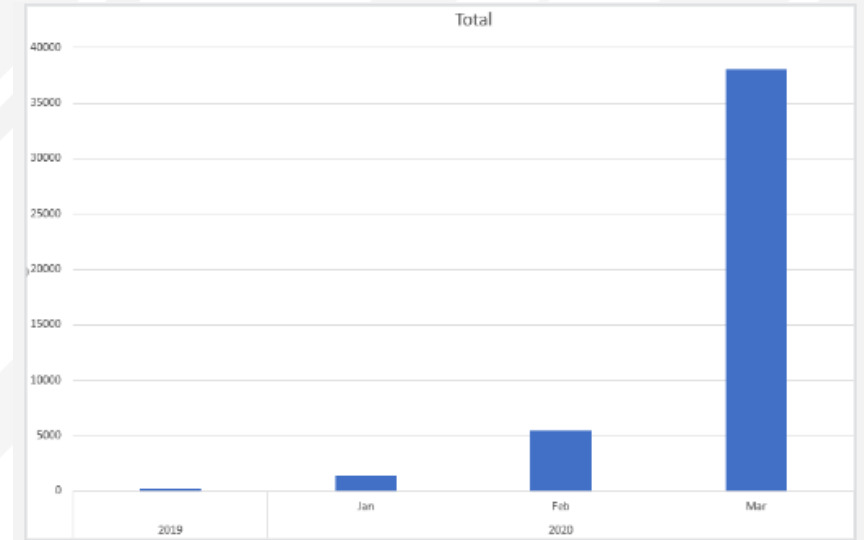


Figure 1: Graph showing the increase in phishing domain registrations related to COVID-19 between December 2019 and March 2020. Source: IntSights Threat Command

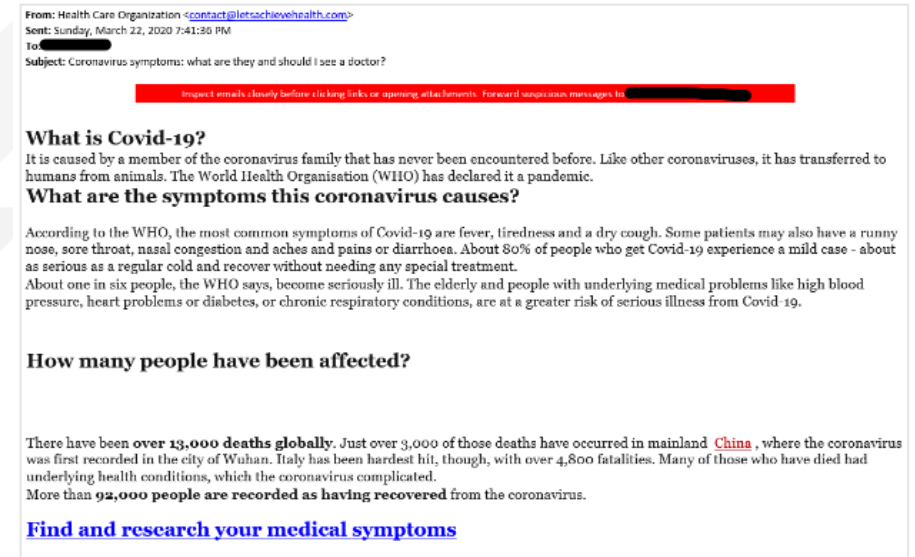
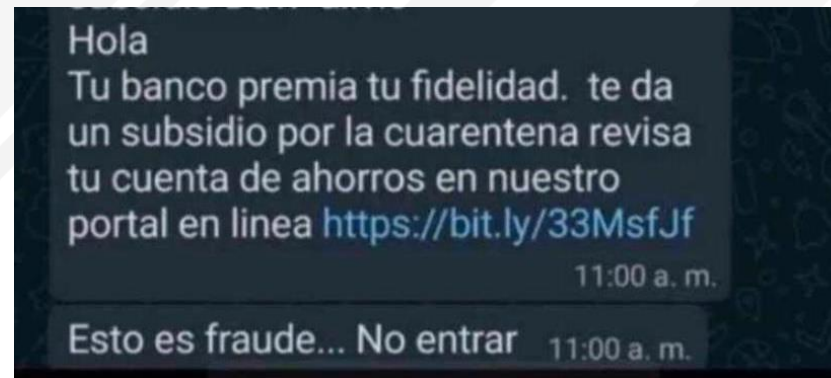


Figure 2: A phishing email that impersonates DHS and redirects victims to a malware download address

Tácticas, Herramientas y Procedimientos

- Extorsión y Miedo

What do I know about you?

To start with, I know all of your passwords. I am aware of your whereabouts, what you eat, with whom you talk, every little thing you do in a day.

What am I capable of doing?

If I want, I could even infect your whole family with the CoronaVirus, reveal all of your secrets. There are countless things I can do.

What should you do?

You need to pay me \$4000. You'll make the payment via Bitcoin to the below-mentioned address. If you don't know how to do this, search "how to buy bitcoin" in Google.

Bitcoin Address:

(It is cAsE sensitive, so copy and paste it)

You have 24 hours to make the payment. I have a unique pixel within this email message, and right now, I know that you have read this email.

If I do not get the payment:

I will infect every member of your family with the CoronaVirus. No matter how smart you are, believe me, if I want to affect, I can. I will also go ahead and reveal your secrets. I will completely ruin your life.

Nonetheless, if I do get paid, I will erase every little information I have about you immediately. You will never hear from me again. It is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Figure 11: [Source](#)

Tácticas, Herramientas y Procedimientos

- Fraude

FAST CORONAVIRUS DETECTOR \$400

Vendor: [Rodrigomendez](#) (82.6)

WICKR.....

RODRIG45
RODRIG45
RODRIG45



FAST DETECTOR OF CORONAVIRUS
YOU NEED EVEN FOR YOUR HOME USE OR MORE

FOR FASTER RESPONDS AND MORE INFO'S ABOUT PRODUCT ... CONTACT

WICKR.....

RODRIG45
RODRIG45
RODRIG45

Price: \$ 0.061738 (400.00000000 USD)

S & H:

• fedex

GET THAT VACCINE FOR THE MOST VIRAL CORONA VIRUS

Vendor: [Legashop](#) (98.4)

PROMOTION, PROMOTION, PROMOTION.

Welcome Valued Clients Buy tested and trusted corona vaccine against the wide spread deadly pandemic virus called corona virus putting threads on lives at comfortable and affordable prices 100% DELIVERY GUARANTEE WITH UPS DHL USPS. FAST DISCREET OVERNIGHT DELIVERY WITHIN THE USA AND STEALTH DELIVERY WORLDWIDE. WE ALSO DO PROVIDE TRACKING DETAILS ONCE PACKAGE IS REGISTER. WE ARE AVAILABLE 24/7

CUSTOMERS SATISFACTION IS OUR TOP PRIORITY AS WE LOOK FORWARD TO BUILD AND DO LONG TERM BUSINESS.

PLEASE all new clients do contact us through our wickr app or whatsapp number below for FAST AND EASY Communication

Wickr ID: legashop247

Whatsapp number: +14089091479

Price: \$ 0.069455 (450.00000000 USD)

S & H:

- UPS
\$ 0.003859 (25.00000000 USD)
- DHL
\$ 0.003859 (25.00000000 USD)
- USPS
\$ 0.003859 (25.00000000 USD)

Accepted Crypto Currencies:

Bitcoin, Dash, Litecoin, BitcoinCash, Vericon, Monero

Ships From: United States

Ships To: Worldwide



Figure 14: Source - hxxp://agarthafidkiwas.onion/Item/6590149416587138941

Other > Drug Test Kits

New rapid test kit to detect COVID-19

Vendor: [CannaCare](#) (99.3)

This test kit, which has been developed and is manufactured by Curis' strategic partner BIGI in Shenzhen, China, enables diagnostic laboratories to test for SARS-CoV2, the virus causing COVID-19, in only a matter of hours.

The kit contains enough reagents and controls to test up to 48 patients in just a few hours

wickr id: CannaCare79

Price: \$ 0.123476 (800.00000000 USD)

S & H:

- priority shipping
\$ 0.002315 (15.00000000 USD)
- express mail
\$ 0.003087 (20.00000000 USD)
- 24hour overnight delivery
\$ 0.006946 (45.00000000 USD)

Accepted Crypto Currencies:

Bitcoin

Ships From: United States

Ships To: Worldwide

Figure 12: Source - http://

OWN SHOP

Best Marketplaces to Buy & Sell Online

Shop

Checkout

My account

Become a Vendor

Vendor Dashboard

Checkout

Contact us

\$0.00 0 items

Home > Promotions > Coronavirus - COVID-19



Coronavirus - COVID-19

\$1,000.00

I was infected with Coronavirus - COVID-19

I sell my infected blood and saliva.

I do this to provide for my family financially.

Indicate how you prefer to get after purchase-Order notes (optional).

1 Add to cart

Sold By: COVID-19

Currency: Dollars, Euros

Tags: Corona, Coronavirus, COVID-19, Virus

Product categories:

- Advertisine
- Air Shipping
- Carding
- Counterfeits
- Digital Downloads
- Instruments
- Drugs
- Electronics
- Gift Cards
- Hacks
- Health
- Potions, Viruses
- Saboteur Kits
- Sex-Only Services
- Shop, More

Figure 16: Source - hxxp://ownshoppar25ghcs.onion/?product=coronavirus-covid-19

Tácticas, Herramientas y Procedimientos

- Aplicaciones Móviles

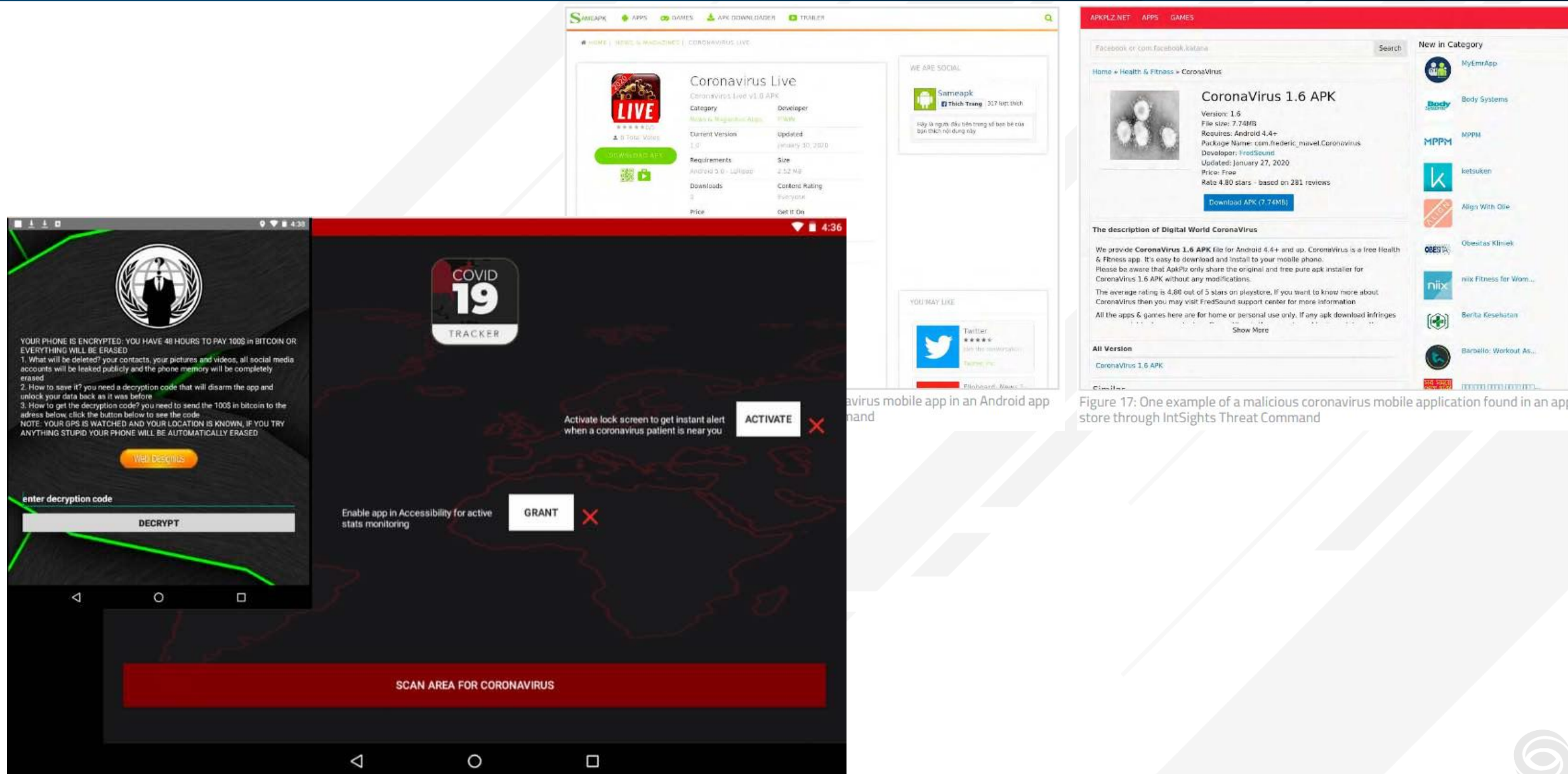


Figure 17: One example of a malicious coronavirus mobile application found in an app store through IntSights Threat Command



Recomendaciones:

- Uso de inteligencia de amenazas.
- Monitoreo continuo de tecnologías de acceso remoto y colaboración con sus respectivas vulnerabilidades. Incluyendo repositorios de código.
- Contraseñas, 2FA, enforzar el uso de VPNs y encriptación para comunicación y movimiento de archivos.
- Crear conciencia





Muchas Gracias

Manuela Jaramillo • Comercial para América Latina
manuela@intsights.com