Análisis de actualidad:

Ciberataques enero 2021

Cibercrimen

Entre las noticias destacables en el ámbito del cibercrimen, cabe destacar sendas acciones policiales coordinadas contra dos de las infraestructuras más relevantes de los últimos tiempos: la botnet EMOTET y la plataforma de Ransomware-as-a-Service Netwalker.

Así pues, Europol se hacía eco el 27 de enero de una acción internacional coordinada con la intervención de autoridades policiales y judiciales de varios países para cerrar y tomar el control de una de las botnets más relevantes de la última década: EMOTET.

EMOTET ha sido uno de los servicios de ciberdelincuencia más avanzados, organizados y longevos hasta el momento. Identificado por primera vez como un troyano bancario en 2014, el malware evolucionó hasta convertirse en la solución de referencia para los ciberdelincuentes a lo largo de los últimos años.

La infraestructura de EMOTET ha actuado esencialmente como un malware de primera etapa y "loader" a escala global. Una vez establecido un acceso no autorizado y generado persistencia en el sistema infectado, su forma única de infectar otros equipos en la misma red mediante movimientos laterales lo popularizó en el mundo del cibercrimen. Tras la infección de los sistemas de las víctimas, el acceso a las mismas era vendido por los operadores a otros grupos para implementar cadenas de ataque posteriores, como el robo de datos y la extorsión a través de ransomware, lo que popularizó las cadenas de ataque combinadas con TrickBot y Ryuk entre otros.

La infraestructura de EMOTET estaba compuesta por varios cientos de servidores ubicados en todo el mundo, todos ellos con diferentes funcionalidades para administrar los equipos infectados de las víctimas, propagándose a otras nuevas y, en última instancia, haciendo su botnet más resistente contra los intentos de eliminación.

El mismo día, el 27 de enero, El Departamento de Justicia de EEUU anunció una acción coordinada internacional contra la infraestructura usada por el grupo Netwalker, que se ha saldado con la incautación de cerca de 500.000 $ en criptodivisas, la desactivación de la web alojada en la darkweb empleado por el grupo para comunicarse con sus víctimas y el arresto de un ciudadano canadiense, Sebastien Vachon-Desjardins, que obtuvo unas ganancias aproximadas de 27,6 millones de dólares, actuando como afiliado de la plataforma de ransomware-as-a-service (RaaS) NetWalker.

El modelo de afiliación RaaS de Netwalker ha sido uno de los más prolíficos, en el que los afiliados "alquilan" el uso de una cepa de ransomware en particular de sus creadores o administradores, quienes a cambio obtienen una parte de cada rescate bajo un modelo de *revenue-sharing*.

Según indican algunas fuentes, hay cuatro roles que reciben ingresos de los ataques de NetWalker: el administrador o desarrollador (8-10%), el afiliado (76-80%) y dos roles con comisión adicional (2.5% -5% cada uno).

EMOTET takedown

EUROPOL

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Participating law enforcement authorities:

- Netherlands (Politie)
- Germany (Bundeskriminalamt)
- France (Police Nationale)
- Lithuania (Lietuvos kriminalinės policijos biuras)
- Canada (Royal Canadian Mounted Police)
- USA (Federal Bureau of Investigation)
- UK (National Crime Agency)
- Ukraine (Національна поліція України)

EUROPOL

How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

Emotet opened doors for:

Information stealers

Trojans

Ransomware

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

What made Emotet so dangerous?

Long lasting	Started as a banking Trojan in 2014, evolving over time.
Go-to-solution for criminals	It acted as a door opener for other computers, allowing unauthorised access to other malware families.
Polymorphic	It changed its code each time it was called up.
Resilient	Unique way of infecting networks by spreading the threat after gaining access to just a few devices in the network.

Protect yourself from malware

Always check your emails carefully and watch out for:

attachments or embedded links from unknown senders.

messages with a sense of urgency asking you to download something.

offers with a promise of reward that sounds too good to be true.

Un afiliado, como Vachon-Desjardins, generalmente es responsable de obtener acceso a la red de víctimas y de implementar el malware.

Según las autoridades estadounidenses, NetWalker ha impactado al menos a 305 víctimas de 27 países diferentes, incluidas 203 en los EE. UU.

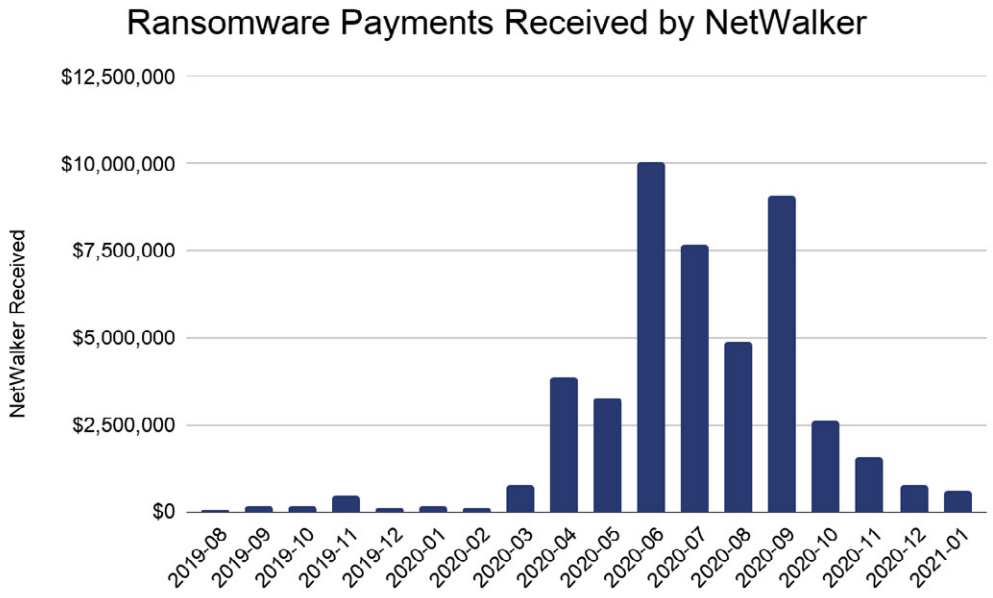


Ilustración 1. Pagos de rescates asociados a Netwalker en los dos últimos años

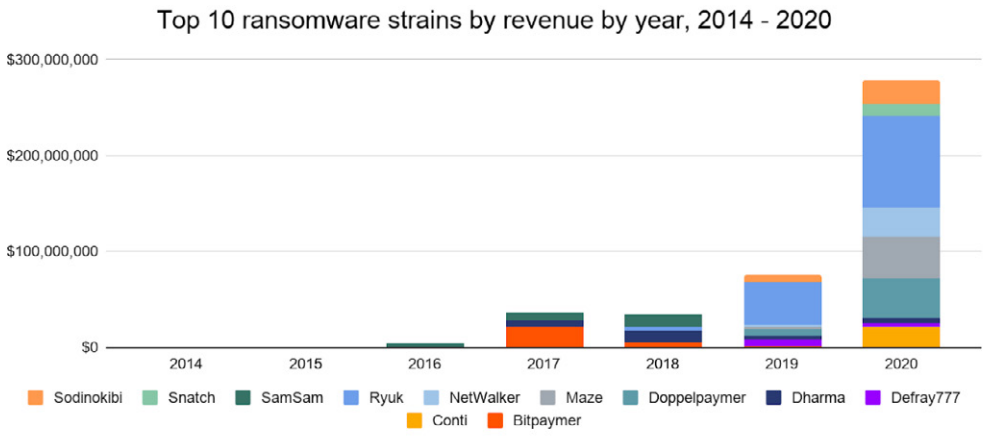


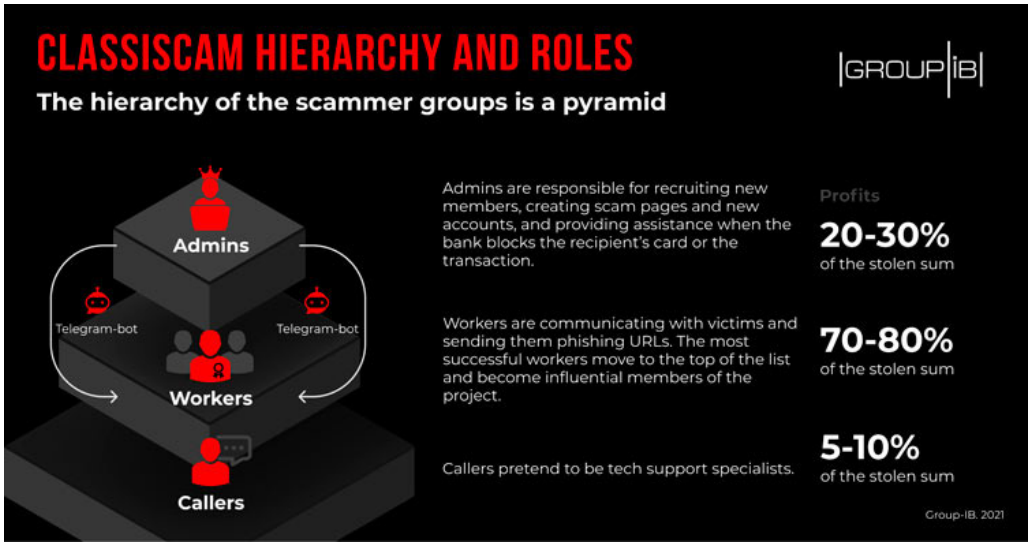
Ilustración 2. Ingresos por rescates de los principales operadores de ransomware

Finalmente, en un informe publicado a mediados de enero, Group-IB publicó haber descubierto una red de fraude en servicios online de anuncios clasificados. El esquema de fraude, denominado Classiscam, es un sistema de scam-as-a-service automatizado diseñado para robar dinero y datos de pago. El esquema utiliza bots de Telegram que brindan a los estafadores páginas listas para usar que imitan las webs de anuncios clasificados más populares, markets online y, a veces, los servicios de paquetería.

Más de 20 grandes grupos, aprovechando el esquema, operan actualmente en Bulgaria, República Checa, Francia, Polonia, Rumania, Estados Unidos y países bálticos, mientras que 20 grupos adicionales trabajan en Rusia. Estos 40 grupos en total se hicieron con más de 6,5 millones de dólares en 2020. Los estafadores están abusando activamente de las marcas de clasificados y mercados internacionales populares, como Leboncoin, Allegro, OLX, FAN Courier, Sbazar, etc.

Como parte de la operación, los estafadores publican anuncios cebo en las mencionadas webs. Los anuncios suelen ofrecer cámaras de fotos, videoconsolas, portátiles, smartphones y artículos similares a precios deliberadamente bajos. El comprador se pone en contacto con el vendedor, quien induce al primero a continuar la conversación a través de una plataforma de mensajería como WhatsApp. Cabe destacar que, para añadirle realismo y popular los anuncios cebo, los estafadores se hacen pasar por compradores y vendedores. Para ser más persuasivos, los estafadores usan números de teléfono locales cuando hablan con sus víctimas. piden a las víctimas que proporcionen su información de contacto para supuestamente organizar una entrega. Luego, el estafador envía al comprador una URL a una web con un formulario de pago fraudulento.

Los analistas advierten que este modelo está creciendo rápidamente y llegando a usuarios de clasificados y markets online europeos, elegidos como objetivo por estafadores de habla rusa para aumentar sus ganancias y reducir el riesgo de ser detenidos.



Ciberespionaje

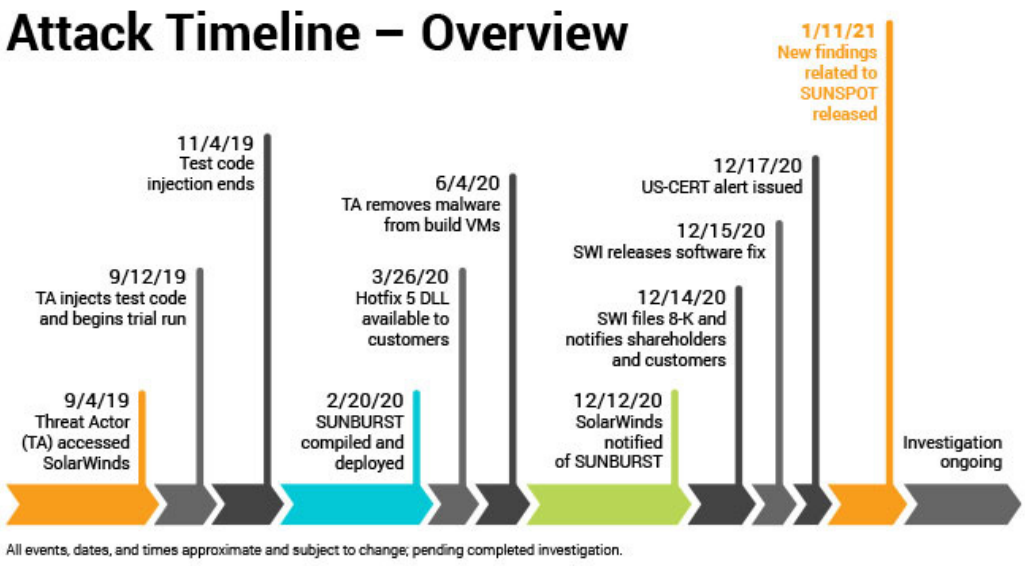
El domingo 13 de diciembre, se hizo público que SolarWinds, empresa de software de gestión IT con sede en Austin, se vio afectada por un ciberataque sobre su cadena de suministro, comprometiendo las actualizaciones de su solución software llamada Orion.

Orion proporciona supervisión centralizada para todo el stack TI de una organización, incluida la red, las operaciones TIC y los productos de seguridad. Entre sus clientes, más de 33.000, se incluyen casi todas las empresas que integran la lista de Fortune 500 y organizaciones gubernamentales de Estados Unidos como la NASA, las fuerzas aéreas o el Pentágono.

Como parte de este ataque, los atacantes insertaron su propio backdoor, denominado Sunburst o Solorigate, en las actualizaciones, que se distribuyeron a muchos clientes de la solución Orion desde por lo menos mes de septiembre de 2019.

La versión de la plataforma Orion lanzada posteriormente a octubre de 2019, parece mostrar contenido malicioso introducido por los atacantes para verificar la capacidad de acceso remoto en las releases recién publicadas. El artefacto malicioso SUNBURST fue detectado en las versiones Orion a partir del 20 de febrero de 2020. Durante todo ese periodo, los atacantes no fueron detectados en los sistemas y redes de SolarWinds, y eliminaron el malware desplegado (SUNBURST) de su entorno en junio de 2020. Durante ese tiempo, y tras los primeros análisis técnicos de diciembre de 2020, diversas compañías han reportado actividad ilegítima en sus sistemas con un patrón similar, todas ellas usuarios de Orion, siendo la firma de ciberseguridad FireEye el primero en reportarlo, seguido de otras compañías como Microsoft ty.5 56.

Se ha especulado abiertamente sobre la autoría del que es considerado el mayor ataque sobre la cadena de suministro hasta la fecha. El gobierno de EEUU así como muchos



expertos del sector privado han manifestado la creencia de que un actor estatal extranjero llevó a cabo esta operación como parte de un ataque generalizado contra la infraestructura cibernética norteamericana. Hasta la fecha, las investigaciones no han revelado de forma fehaciente la identidad de los atacantes, si bien el ex secretario de Estado de la administración Trump, Mike Pompeo, apunta abiertamente una autoría rusa.

La investigación realizada hasta el momento por SolarWinds sugiere que, dado que la intrusión en sus sistemas fue ejecutada a través de múltiples servidores basados en territorio norteamericano, imitando el tráfico de red legítimo, los atacantes pudieron así eludir las técnicas de detección de amenazas empleadas por la compañía, otras empresas privadas de seguridad y el propio gobierno federal.

El 5 de enero, el FBI, el CISA, ODNI y NSA emitieron una declaración conjunta en la que dijeron que su investigación hasta ahora indicaba que "un actor de APT, probablemente de origen ruso, es responsable para la mayoría o todos los compromisos cibernéticos en curso y recientemente descubiertos de las redes gubernamentales y no gubernamentales. En este momento, creemos que esto fue, y sigue siendo, un esfuerzo de recopilación de inteligencia".

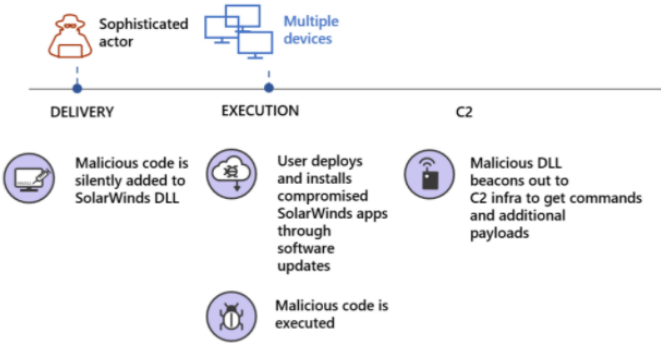


Ilustración 3. Diagrama de funcionamiento por etapas de Solorigate

JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA)

Original release date: January 05, 2021

On behalf of President Trump, the National Security Council staff has stood up a task force construct known as the Cyber Unified Coordination Group (UCG), composed of the FBI, CISA, and ODNI with support from NSA, to coordinate the investigation and remediation of this significant cyber incident involving federal government networks. The UCG is still working to understand the scope of the incident but has the following updates on its investigative and mitigation efforts.

This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks. At this time, we believe this was, and continues to be, an intelligence gathering effort. We are taking all necessary steps to understand the full scope of this campaign and respond accordingly.

The UCG believes that, of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number have been compromised by follow-on activity on their systems. We have so far identified fewer than ten U.S. government agencies that fall into this category, and are working to identify and notify the nongovernment entities who also may be impacted.

This is a serious compromise that will require a sustained and dedicated effort to remediate. Since its initial discovery, the UCG, including hardworking professionals across the United States Government, as well as our private sector partners have been working non-stop. These efforts did not let up through the holidays. The UCG will continue taking every necessary action to investigate, remediate, and share information with our partners and the American people.

As the lead agency for threat response, the FBI's investigation is presently focused on four critical lines of effort: identifying victims, collecting evidence, analyzing the evidence to determine further attribution, and sharing results with our government and private sector partners to inform operations, the intelligence picture, and network defense.

As the lead for asset response, CISA is focused on sharing information quickly with our government and private sector partners as we work to understand the

Ilustración 4. Declaración conjunta de diversos agentes gubernamentales sobre la autoría del ataque a SolarWinds

SolarWinds' Customers

SolarWinds' comprehensive products and services are used by more than 300,000 customers worldwide, including military, Fortune 500 companies, government agencies, and education institutions. Our customer list includes:

- More than 425 of the US Fortune 500
- All ten of the top ten US telecommunications companies
- All five branches of the US Military
- The US Pentagon, State Department, NASA, NSA, Postal Service, NOAA, Department of Justice, and the Office of the President of the United States
- All five of the top five US accounting firms
- Hundreds of universities and colleges worldwide

Partial customer listing:

Acxiom
Ameritrade
AT&T
Bellsouth Telecommunications
Best Western Intl.
Blue Cross Blue Shield
Booz Allen Hamilton
Boston Consulting
Cable & Wireless
Cablecom Media AG
Cablevision
CBS
Charter Communications
Cisco
CitiFinancial
City of Nashville
City of Tampa
Clemson University
Comcast Cable
Credit Suisse
Dow Chemical
EMC Corporation
Ericsson
Ernst and Young
Faurecia
Federal Express
Federal Reserve Bank
General Dynamics
Gillette Deutschland GmbH
GTE
H&R Block
Harvard University
Hertz Corporation
ING Direct
IntelSat
J.D. Byrider
Johns Hopkins University
Kennedy Space Center
Kodak
Korea Telecom
Leggett and Platt
Level 3 Communications
Liz Claiborne
Lockheed Martin
Lucent
MasterCard
McDonald's Restaurants
Microsoft
National Park Service
NCR
NEC
Nestle
New York Power Authority
New York Times
Sabre
Saks
San Francisco Intl. Airport
Siemens
Smart City Networks
Smith Barney
Smithsonian Institute
Sparkasse Hagen
Sprint
St. John's University
Staples
Subaru
Supervalu
Swisscom AG
Symantec
Telecom Italia
Telenor
Texaco
The CDC
The Economist
Time Warner Cable
U.S. Air Force
University of Alaska
University of Kansas
University of Oklahoma
US Dept. Of Defense
US Postal Service

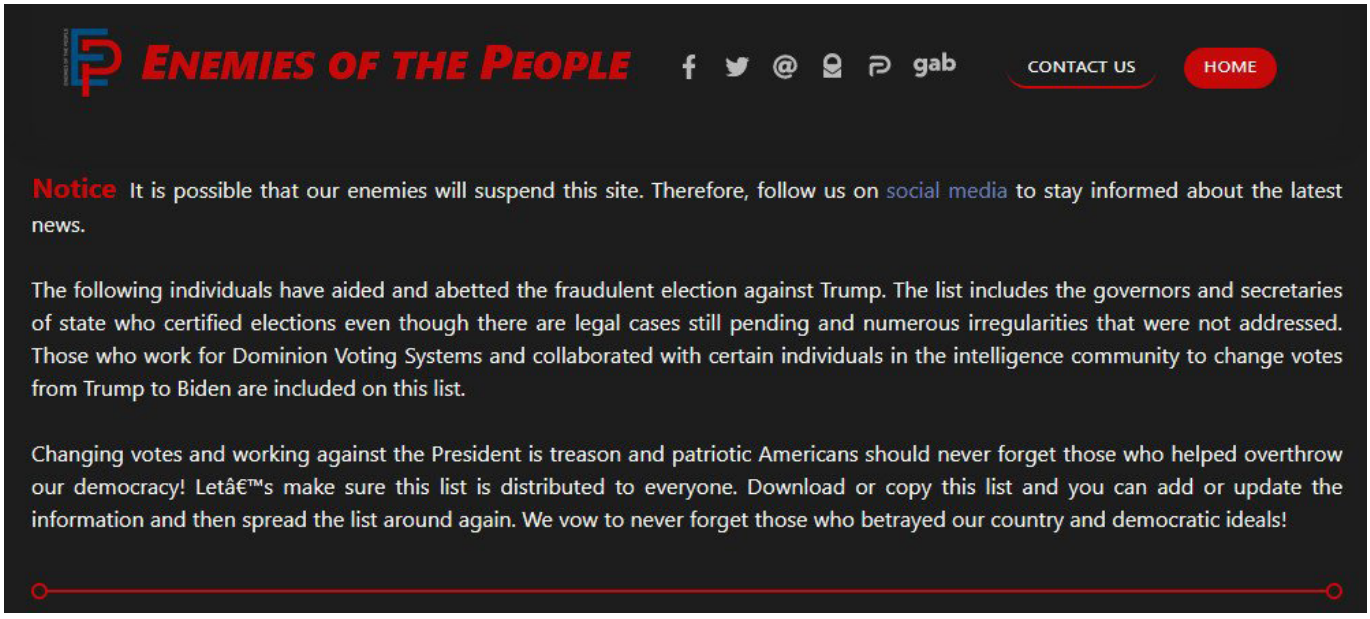
Hacktivismo, guerra electrónica y operaciones de información

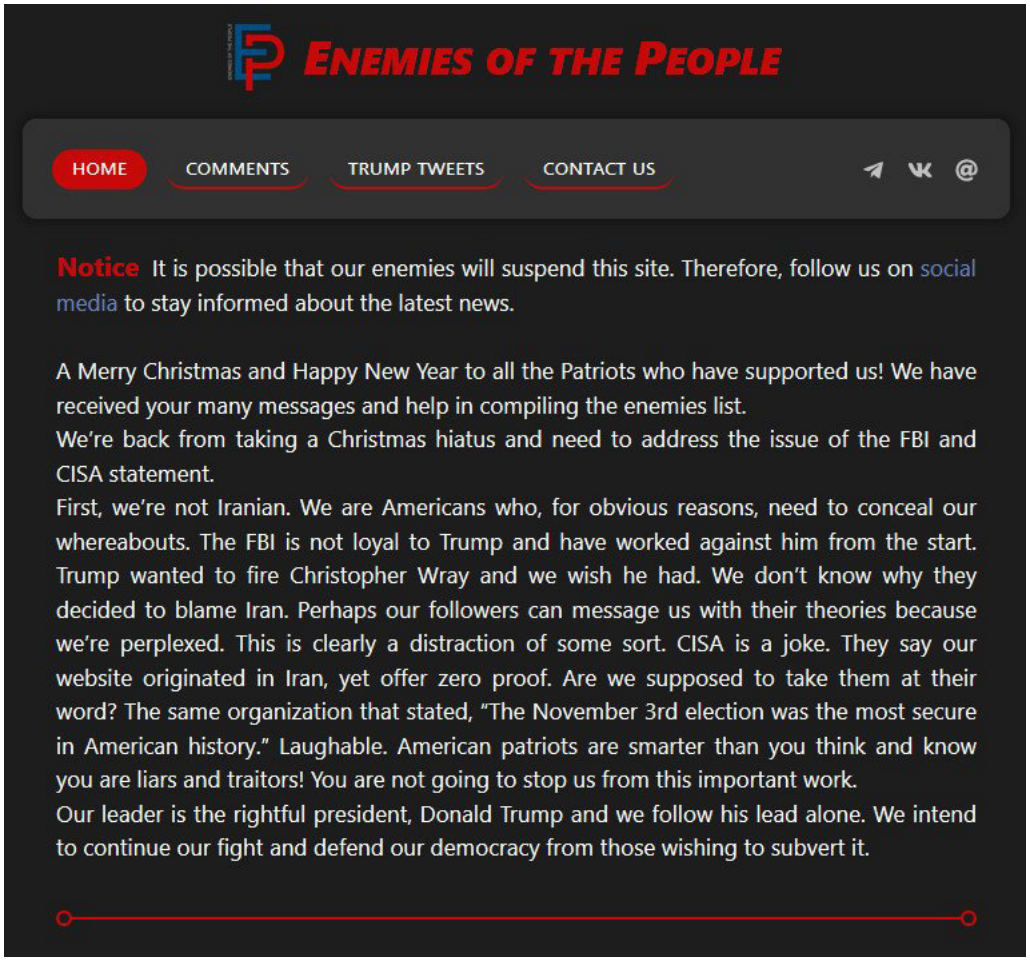
El uso del ciberespacio como medio para realizar campañas de información y hacktivismo durante los últimos dos meses, ha estado fuertemente marcado por la cita electoral norteamericana.

Así pues, El FBI y el CISA estadounidense, a finales de diciembre del año pasado, indicaron poseer información fiable relativa a la actividad de unos actores iraníes vinculados a una web denominada "Enemies of the People", en la que vertían amenazas de muerte dirigidas a funcionarios electorales estadounidenses.

El FBI identificó múltiples dominios, siendo el principal www.enemigosofthepeople.org (actualmente inactivo), que contenía información personal y fotografías de varios funcionarios estadounidenses y personas relevantes del sector privado involucradas en los comicios.

La creación postelectoral de la web Enemies of the People demuestra potencialmente la intención iraní de crear divisiones y desconfianza en EEUU socavando la confianza pública en el proceso electoral.



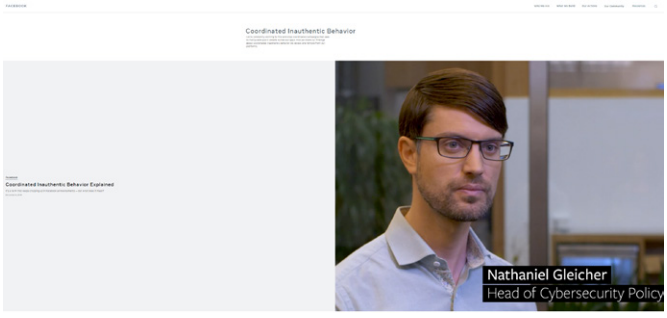


Ilustraciones 5 y 6.
enemigosofepeople.org

Finalmente, ya a mediados de enero, Facebook confirmó la eliminación durante el mes de diciembre de más de 2.000 cuentas, páginas y grupos falsos asociados a diversos países, algunos de los cuales tenían como objetivo las elecciones estadounidenses, tratando de suplantar a medios de comunicación entre otros. Esta actividad de takedowns mensual por parte de Facebook ha sido la más intensa registrada.

El gigante de las redes sociales se ha visto sometido a mucha presión para que adquiriese una postura más proactiva contra las fake-news y los perfiles falsos tras las elecciones presidenciales de 2016, en la que trolls rusos usaron sus plataformas para interferir en el proceso electoral. El escrutinio de la compañía se ha intensificado aún más desde el incidente en el Capitolio el pasado 6 de enero.

La compañía confirmo que durante diciembre eliminó 1.957 cuentas de Facebook, 707 cuentas de Instagram, 156 páginas y 727 grupos por engañar a los usuarios sobre su propósito e identidad. Se eliminaron 14 redes de cuentas falsas no detectadas hasta la fecha, procedentes de Irán, Marruecos, Ucrania, Kirguistán, Argentina, Brasil, Pakistán e Indonesia. La red social también eliminó cuentas falsas de Rusia y Francia. La mayoría de las operaciones se centraron en las elecciones y muestran una clara orientación a usuarios locales.



La red más grande que Facebook eliminó en diciembre provino de Argentina. La compañía eliminó 663 cuentas de Facebook y 388 cuentas de Instagram de ese país. Las cuentas falsas utilizaron inteligencia artificial para generar perfiles falsos y en su mayoría promocionaron publicaciones y artículos en español sobre el ministro de Seguridad de Buenos Aires, Sergio Berni.

Según se desprende del propio informe de Facebook, las campañas nacionales como las identificadas plantean un desafío complejo al difuminar la línea entre el debate saludable y la manipulación.