



Miguel Gallardo <miguel902998352@gmail.com>

Secretaria de Estado de Justicia, Carmen Sánchez-Cortés Martín Cc: Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional, Félix Sanz Roldán en documento con firma digital publicado en www.cita.es/claves-lexnet.pdf

apedanica ong <apedanica.ong@gmail.com> 7 de agosto de 2018, 11:38

Para: SECRETARIA.ESTADO@mjusticia.es, sgajus@mjusticia.es, subsecretaria@mjusticia.es, sgcontratacionyservicios.secretaria@mjusticia.es

Cc: acreditacion.ccn@cni.es, ccn-cert@ccn-cert.cni.es, ccn-cert@cni.es, ccn@cni.es, cni@cni.es, daocni@cni.es, emsec.ccn@cni.es, estudioHTTPS@ccn-cert.cni.es, incidentes@ccn-cert.cni.es, ines@ccn-cert.cni.es, info@ccn-cert.cni.es, organismo.certificacion@cni.es, redsara@ccn-cert.cni.es, sat-inet@ccn-cert.cni.es, sat-sara@ccn-cert.cni.es, sondas@ccn-cert.cni.es

Cco: miguelangel.gallardo@ucm.es

Dr. (PhD) Miguel Gallardo PERITO JUDICIAL Tel. (+34) 902998352 E-mail: apedanica.ong@gmail.com

Asociación APEDANICA con registro en el Ministerio del Interior publicado en www.cita.es/apedanica.pdf

Secretaria de Estado de Justicia, Carmen Sánchez-Cortés Martín

Cc: Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional, Félix Sanz Roldán en [documento con firma digital publicado](http://www.cita.es/claves-lexnet.pdf) en www.cita.es/claves-lexnet.pdf

Considerandola Resolución de 26 de julio de 2018, de la Subsecretaría, por la que se publica el Convenio en materia de ciberseguridad entre el Ministerio de Justicia y el Centro Nacional de Inteligencia en el «BOE» núm. 181, de 27 de julio de 2018 https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-10637

Como mejor proceda ponemos en su conocimiento que un abogado nos ha confiado un grave incidente de seguridad en LexNET porque recibió el correo electrónico (adjunto) con su clave de acceso a LexNET pidiéndole 7.000 dólares en BITCOINS en el monedero "1KRjNsfNwuK86YCaPhQnDmEGEbuPvzuRU8". Con ese mensaje de extorsión se evidencia que pueden obtenerse claves LexNET también de jueces, fiscales y funcionarios judiciales.

Y considerando también que el Centro Criptológico Nacional C.C.N. del Centro Nacional de Inteligencia C.N.I. cuenta con el Equipo de Respuesta a incidentes de Seguridad de la Información del C.C.N., que tiene responsabilidad en los ataques procedentes del ciberespacio sobre sistemas del sector público y que la citada resolución incluye **detección de incidentes en los sistemas de la S.G.N.T.J y se optimizará la capacidad de reacción y respuesta ante cualquier ataque, de conformidad con los criterios e información suministrada por la S.G.N.T.J.**

La asociación **APEDANICA** solicita a quien corresponda información y un interlocutor funcionario experto en incidentes de seguridad en LexNET, especialmente en cuanto pudiera haber comprometido la claves de acceso de

sus usuarios. Por lo que nos ha comentado el abogado que recibió el correo adjunto, existe la posibilidad de que empleados públicos o de **empresas relacionadas con LexNET (como ISDEFE, INDRA, AVALON, SERMICRO, SATEC, INDRA, IECISA y NOVASOFT, entre otras)** hayan hecho uso negligente o indebido de claves de acceso a LexNET, o bien que exista un “malware” capaz de averiguar esas clave, como dice el correo adjunto. Tanto si hubo acceso general, como si fue individual, **LexNET parece estar en grave riesgo.**

La asociación **APEDANICA** tiene el máximo interés pericial por conocer todo cuanto sea posible de cualquier delito en el que afecte a LexNET o en el que se utilicen BITCOINS y muy especialmente, de extorsiones, coacciones o chantajes que exijan pagos en BITCOINS. Yo, además, tengo razones científicas doctrinales, y alguna muy personal, para investigarlos, pues mi tesis doctoral de 2015 se tituló **“PROBLEMAS MORALES DE LAS INTRUSIONES, GRABACIONES Y ESCUCHAS. HACIA UNA ÉTICA DEL DESCUBRIMIENTO Y LA REVELACIÓN DE SECRETOS”** según puede verse en www.miguelgallardo.es/tesis.pdf y he publicado numerosos artículos sobre criptología y seguridad. **APEDANICA** se ofrece a todos los que hayan recibido mensajes parecidos para agotar todas las posibilidades legales de identificación de extorsionadores en cualquier país, haciendo responsables civiles a todos los que aportan algún elemento útil para su extorsión. Tenemos algunas **hipótesis periciales que preferimos no publicar todavía.** No podemos descartar que el incidente de seguridad que evidencia del correo electrónico sea un hecho aislado personal, particular y privado de un único abogado, o por el contrario, que todas claves de acceso a LexNET, incluyendo las de jueces y fiscales, hayan sido comprometidas.

APEDANICA solicita audiencia con el funcionario más competente para la investigación de los hechos porque entendemos que se trata de un incidente de seguridad en LexNET que puede afectar a muchos abogados y procuradores (y también a terceros que les confían sus asuntos o incluso a quienes son mencionados en documentos judiciales sin ser parte) cuyas claves de acceso puedan haberse comprometido, en cuyo caso, entendemos que existe la obligación de notificar las quiebras de seguridad y sobre ello, **solicitamos información por la Ley 19/2013, al menos, sobre las categorías y las estadísticas de los incidentes de seguridad en LexNET y un interlocutor que sea competente en S.G.N.T.J-C.C.N.-C.E.R.T.** pues estamos desarrollando contramedidas y tecnologías que evidencien pericialmente que existen organizaciones criminales internacionales que envían mensajes como el delictivo que adjuntamos suprimiendo, únicamente, los datos de quien nos ha confiado su problema (para quien pedimos la máxima protección legal, y absoluta confidencialidad), permitiéndonos publicar esto:

----- Forwarded message -----

From: **Ignacio Alhberg** <facornellzkw@hotmail.com>

Date: T1 Subject: S1 To: X1

It is just so unfortunate. I do know P1 is your password. More importantly, I do know about your secret and I've evidence of this. You don't know me personally and nobody hired me to examine you.

It is just your misfortune that I came across your misdemeanor. The truth is, I actually setup a malware on the adult videos (sexually graphic) and you visited this website to have fun (you know what I mean). When you were busy watching video clips, your browser began working as a Rdp (Remote control desktop) with a key logger which provided me with accessibility to your screen and webcam. Just after that, my software gathered all your contacts from facebook, and mailbox.

After that I put in much more hours than I probably should've looking into your life and created a two view video. First part shows the video you had been watching and next part displays the view from your webcam (its you doing nasty things).

Frankly, I'm ready to forget everything about you and let you continue with your life. And I am about to provide you two options which will accomplish that. These two choices to either ignore this letter, or simply just pay me \$7000. Let's explore those 2 options in details.

Option One is to ignore this e-mail. Let me tell you what is going to happen if you pick this path. I will, no doubt send your video recording to all your contacts including members of your family, co-workers, and so forth. It will not save you from the humiliation your self will have to face when friends uncover your unpleasant details from me.

Other Option is to make the payment of \$7000. We'll call it my "privacy tip". Let me tell you what happens if you opt this option. Your secret will remain your secret. I will erase the recording immediately. You keep your routine life as though nothing ever happened.

Now you must be thinking, "I will call the cops". Let me tell you, I've covered my steps to ensure this email message can't be tracked returning to me plus it won't stop the evidence from destroying your daily life. I am not seeking to break your bank. I just want to get paid for efforts and time I put in investigating you. Let's hope you decide to create all of this disappear completely and pay me the confidentiality fee. You'll make the payment through Bitcoin (if you don't know how, search "how to buy bitcoins" on google search)

Required Amount: \$7000

Receiving Bitcoin Address: 1KRjNsfNwuK*86YCaPhQnDmEGEbuPvzuRU8 (Remove * from this address then note it)

Expalin no-one what you will be sending the bitcoin for or they possibly will not sell it to you. The method to obtain bitcoins may take a few days so do not wait.

I have a special pixel within this mail, and at this moment I know that you've read this e-mail. You have 2 days to make the payment. If I don't receive the BitCoin, I will send your video recording to your entire contacts including friends and family, colleagues, and so on. You better come up with an excuse for friends and family before they find out. Nevertheless, if I receive the payment, I will erase the recording and all other proofs immediately. It's a non negotiable one time offer, so please don't ruin my personal time & yours. Your time is running out. Please note that, my malware will still be sharing what action you adopt when you're done looking over this message. To be honest, If I see any wrong activity from your search history then I will send your video recording to your relatives, coworkers before time ends.

Más información:

[Dr. \(PhD\) Miguel Gallardo PERITO JUDICIAL](#) Tel. (+34) 902998352 E-mail: **apedanica.ong@gmail.com**

[Asociación APEDANICA](#) con registro en el Ministerio del Interior publicado en **www.cita.es/apedanica.pdf**