Bilaga C

Exempel på abuseärenden

Notera att information om avsändare och annan personlig information är borttagen ur dessa exempel.

Exempel 1 – Copyright Compliance

Notice ID: 22-102071976
Notice Date: 28 Aug 2013 03:56:47 GMT

Foreningen For Digitala Fri- Och Rattigheter

Dear Sir or Madam:

Irdeto USA, Inc. (hereinafter referred to as "Irdeto") swears under penalty of perjury that Paramount Pictures Corporation ("Paramount") has authorized Irdeto to act as its non-exclusive agent for copyright infringement notification. Irdeto's search of the protocol listed below has detected infringements of Paramount's copyright interests on your IP addresses as detailed in the below report.

Irdeto has reasonable good faith belief that use of the material in the manner complained of in the below report is not authorized by Paramount, its agents, or the law. The information provided herein is accurate to the best of our knowledge. Therefore, this letter is an official notification to effect removal of the detected infringement listed in the below report. The Berne Convention for the Protection of Literary and Artistic Works, the Universal Copyright Convention, as well as bilateral treaties with other countries allow for protection of client's copyrighted work even beyond U.S. borders. The below documentation specifies the exact location of the infringement.

We hereby request that you immediately remove or block access to the infringing material, as specified in the copyright laws, and insure the user refrains from using or sharing with others unauthorized Paramount's materials in the future.

Further, we believe that the entire Internet community benefits when these matters are resolved cooperatively. We urge you to take immediate action to stop this infringing activity and inform us of the results of your actions. We appreciate your efforts toward this common goal.

Please send us a prompt response indicating the actions you have taken to resolve this matter, making sure to reference the Notice ID number above in your response.

If you do not wish to reply by email, please use our Web Interface by clicking on the following link:
http://webreply.copyright-compliance.com/WebReply?webreplyhash=860448a13760233fbb94e922a4315ad3

Nothing in this letter shall serve as a waiver of any rights or remedies of Paramount with respect to the alleged infringement, all of which are expressly reserved. Should you need to contact me, I may be reached at the below address.

Regards,

XXX XXX
Irdeto USA, Inc.
3255-3 Scott Blvd. Suite 101 Santa Clara, CA 95054
Phone: 408-492-8500 fax: 408-727-6743
paramount@copyright-compliance.com

*pgp public key is available on the key server at http://pgp.mit.edu

Note: The information transmitted in this Notice is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, reproduction, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from all computers.

This infringement notice contains an XML tag that can be used to automate the processing of this data. If you would like more information on how to use this tag please contact Irdeto.

Evidentiary Information:

Notice ID: 22-102071976
Initial Infringement Timestamp: 28 Aug 2013 03:53:49 GMT
Recent Infringement Timestamp: 28 Aug 2013 03:53:49 GMT
Infringers IP Address: 171.25.193.235
Protocol: BitTorrent
Infringed Work: Star Trek Into Darkness
Infringing File Name: Star.Trek.Into.Darkness.2013.720p.WEB-DL.H264-PublicHD
Infringing File Size: 4443710666
Bay ID: 694b1dd96fdbe673d59b77d1c88a0ee455dc0d72|4443710666
Port ID: 28734
Infringer's User Name:

DFRI:s svar

Hello,

The IP address in question is a Tor exit relay, see https://www.torproject.org/overview.html for more info about the Tor Project.

We do not support any form of copyright infringement. There is however very little we can do to trace this matter further. As can be seen from the overview page, the Tor network is designed to make tracing of users impossible. The Tor network is run by some 3000 volunteers using free software provided by the Tor Project to run Tor relays. Client connections are routed through multiple relays. The system does not record logs of client connections or previous hops.

To tell if a Tor exit relay is running on a given IP address, the Tor Project provides as a service named TorDNSEL: https://www.torproject.org/tordnsel/.

Thank you for your understanding. If you have further questions, feel free to contact us again.

Regards :DFRI Abuse Team

Exempel 2 – Spam av news

Hi,

Thank you for your report. The IP address in question is, as you already seem to know, a Tor exit relay, see https://www.torproject.org/overview.html for more info about the Tor Project.

There is little we can do to trace this matter further. As can be seen from the overview page, the Tor network is designed to make tracing of users impossible. The Tor network is run by some 2500 volunteers using free software provided by the Tor Project to run Tor relays. Client connections are routed through multiple relays. The system does not record logs of client connections or previous hops.

I think that the long term solution is, as you mention in your post, to get Google as the service provider to handle this investigation.

If we block groups.google.com it will have consequences to other users of that service.

If you have further questions, feel free to contact us again.

Regards
:DFRI Abuse Team

On 09/15/2012 10:30 PM, XXX wrote:
> This is some voluminous, off-topic flooding and harassment on the
> ba.broadcast Usenet newsgroup. It is being reported to abuse reporting
> mailboxes based on the contents of the NNTP-Posting-Host: and
> X-Complaints-To: headers, and lookup of the originating IP address via
> WHOIS and the Network Abuse Clearinghouse. They are sometimes also
> crossposted to unrelated newsgroups such as rec.arts.tv,
> soc.culture.new-zealand, and several other newsgroups in the nz.*
> hierarchy. It is disruptive, and completely off-topic, as well as
> causing disruptive, cascaded flame wars among those unrelated
> newsgroups.
>
> This user has also been posting from other sources, including 100tb.com,
> 31173.se, 51.net, 62.net, all.de, armax.me, bahnhof.se, bayern.de,
> boingboing.net, broadviewnet.net, ccc.de, co.at, creekcabin.com,
> exit.de, finalhosting.cz, formlessnetworking.net, hessmo.com,
> hexhost.net, ib.de, ipredator.se, mydev.net, noisetor.net, oceanic.net,
> plebia.org, ovh.net, privacyfoundation.ch, privacyrepublic.org,
> riseup.net, ru.is, sbcglobal.net, scnet.net, servers.com, snydernet.net,
> solidonetworks.com, stanford.edu, stargrave.org, torland.is, torland.me,
> torservers.net, trolling.me, dmzglobal.com, telstraclear.net,
> xtra.co.nz, clear.net.nz, orcon.net.nz, netgate.net.nz,
> freeparking.co.nz, powerusenet.com, giganews.com, thundernews.com,
> altopia.com, comcast.net, groups.google.com, and tigerusenet.com. It
> appears that you are merely the latest of his victims.
>
> The charter of ba.broadcast is as follows:
>
> "This group is here for discussions, comments and program reminders
> about broadcast media in the San Francisco Bay Area, both radio and
> television. It also includes cable systems and TVRO/BCRO in the SF Bay
> Area. It does not include scanner, ham radio or other action here in
> the SF Bay Area; these may be addressed in another newsgroup at another
> time. Issues of national interest should be posted to one of the groups
> in rec.arts.tv or rec.radio."
>
> (see: http://groups.google.com/group/ba.broadcast/browse_thread/thread/ddfbd8175e26286e/d8f642f8a1fc5f42)
>
> The charter does not include sexual innuendo and libel, abusive threats,
> bigotry and minority bashing, or any off-topic discussion of subjects
> not reasonably related to broadcasting in the Bay Area, which now
> consitute the overwhelming majority of current message traffic on
> ba.broadcast, to the detriment and exclusion of on-topic participation
> by others.
>
> Please take appropriate action to put a stop this this misbehavior
> originating from your site that is disrupting ba.broadcast.
>
> Note to TOR Exit Server maintainers:
>
> This article is from Google Groups, a third-party news posting site via
> http (80 port). I have received replies from other TOR exit server
> maintainers that they will temporarily block connectivity to Google
> Groups' range of IP addresses, as this kind of repetitive flooding to
> deny use of a newsgroup is not free speech, and not what the TOR project
> was intended to be used for. The IP addresses for Google Groups are as
> follows:
>
> groups.google.com   canonical name = groups.l.google.com.
> Name: groups.l.google.com
> Address: 74.125.142.102
> Name: groups.l.google.com
> Address: 74.125.142.113

> Name: groups.l.google.com
> Address: 74.125.142.138
> Name: groups.l.google.com
> Address: 74.125.142.139
> Name: groups.l.google.com
> Address: 74.125.142.100
> Name: groups.l.google.com
> Address: 74.125.142.101
>
> Name: googlegroups.com
> Address: 74.125.142.99
> Name: googlegroups.com
> Address: 74.125.142.103
> Name: googlegroups.com
> Address: 74.125.142.104
> Name: googlegroups.com
> Address: 74.125.142.105
> Name: googlegroups.com
> Address: 74.125.142.106
> Name: googlegroups.com
> Address: 74.125.142.147
>
> Google Groups has (typically) been unresponsive, even for the most
> egregious on-line threats and flooding that is supposed to be considered
> abuse by them. They are the ones that would have to implement blocking
> of your exit nodes to stop this flooder. The security practices of
> sites under my control are fine, including blocking of all TOR exit
> servers.
>
> The article quoted below is one of thousands over the past year. I can
> send you far worse examples, if required. A good sampling of the
> perpetrator's mental state, and criminal record, may be found at:
>
> http://www.smbtech.com/ras/
>
> Offending article follows:
>
>
> Received: by 10.224.220.12 with SMTP id hw12mr4584420qab.8.1347738925964;
> Sat, 15 Sep 2012 12:55:25 -0700 (PDT)
> MIME-Version: 1.0
> Received: by 10.236.181.234 with SMTP id l70mr1162960yhm.5.1347738925918; Sat,
> 15 Sep 2012 12:55:25 -0700 (PDT)
> Path: novia.net!newscene!newscene.com!novia!news-out.readnews.com!transit3.readnews.com!
209.85.216.88.MISMATCH!v8no3862778qap.0!news-out.google.com!da15ni67587947qab.0!nntp.google.com!
v8no3862773qap.0!postnews.google.com!d6g2000yqd.googlegroups.com!not-for-mail
> Newsgroups: ba.broadcast,alt.life.sucks
> Date: Sat, 15 Sep 2012 12:55:25 -0700 (PDT)
> Complaints-To: groups-abuse@google.com
> Injection-Info: d6g2000yqd.googlegroups.com; posting-host=171.25.193.21; posting-
account=kDNmQwoAAABrElExtQi-KA7pu1-OmkN9
> NNTP-Posting-Host: 171.25.193.21
> References: <f14aa4e8-0bf5-452e-98f7-515b7088f2e9@v15g2000yqi.googlegroups.com>
> <34e2e33c-5f21-40a0-88f7-95c27c268681@googlegroups.com> <4234e930-14b0-4850-8525-
3878ba894722@v15g2000yqi.googlegroups.com>
> User-Agent: G2/1.0
> X-HTTP-Useragent: Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0,gzip(gfe)
> Message-ID: <5e2550d7-4011-4cc9-b56a-7d49f00f6f77@d6g2000yqd.googlegroups.com>
> Subject: Re: KZSU FM -- Great Deals On L.S.D. Tabs, Coke, Meth, Ice, 420, And
> For The Right Price Will Buy Alcohol For Minors
> From: "Jose' Scott Satanist Drug Dealer Outlaw [kzsu fm]" <zyklon_bozo@37.com>
> Injection-Date: Sat, 15 Sep 2012 19:55:25 +0000
> Content-Type: text/plain; charset=UTF-8
> Content-Transfer-Encoding: quoted-printable
> Xref: novia.net ba.broadcast:284554 alt.life.sucks:442920

>
> KFJC FM (Foothill College): Robert Pelzel's Sandusky Styled
> Alcohol For Minors / Drug Dealers (L.S.D.) C=C2=B2=E2=81=B0H=C2=B2=E2=81=B5=
> N=C2=B3O,
> Drug Users, Drug Pushers At "Devil's Radio"
>
> 'ZERO TOLERANCE'
>
> KFJC FM (Foothill College) LOSES F.C.C. LICENSE:
> DRUG DEALER Jose Scott Admits Doing L.S.D. (C=C2=B2=E2=81=B0H=C2=B2=E2=81=
> =B5N=C2=B3O)
> At Least Twice - Unable To Perform EBS/EAS System
> Endangering Countless Lives
>
> AT KFJC 89.7 FM
> FOOTHILL COLLEGE
> LOS ALTOS HILLS, CALIFORNIA
>
> L.S.D. DRUG DEALERS
> L.S.D. DRUG PUSHERS
> L.S.D. DRUG USERS
> L.S.D. (C=C2=B2=E2=81=B0H=C2=B2=E2=81=B5N=C2=B3O)
>
> DEALING IN MANY OTHER DRUGS!
> I SAID MANY OTHER DRUGS!
> C=C2=B2=E2=81=B0H=C2=B2=E2=81=B5N=C2=B3O
>
> From Website:
> http://www.exorcist.org.nz/the_devils_radio.html
>
> SANDUSKY SYLED ALCOHOLISM:
>
> Under-Age Alcohol Provided, Offered,
> REGULARILY
> By Foothill's KFJC FM Faculty Advisor Moderator:
>
> Robert Edward Pelzel,
> where allegations against him in regards to mail fraud at KFJC
> are documented, through the accusations by ex-station member Anthony
> Ladd, myself and others. Robert Edward Pelzel sees nothing wrong
> with
> the pronounced satanism at KFJC (where he also helps at KALX FM in
> Berkeley) and also provides alcohol to minors at the Boardwalk Bar
> in Los Altos. The Boardwalk is the location of the weekly Wed. after
> station meeting. Robert Edward Pelzel is an alcoholic (is seen
> outdrinking anyone there), and thus provides pitchers of beer to
> those who come down. There is no supervision amongst his purchases
> - while acting as a Foothill College Faculty Advisor. KFJC is a
> drug promoting culture and Robert Edward Pelzel sees nothing wrong
> with what is going down there. Jose' Scott even admitted publicly
> that he took L.S.D. at least twice on the airwaves at KFJC 89.7 FM.
> Jose' called himself: Uncle Sydney. Only he knows why.
>
> ----------
>
> KFJC 89.7 FM
> Foothill Junior College
> Los Altos Hills, California
>
> Drug Dealer Jose Scott Of KFJC FM,
> Admits To Taking L.S.D. At Least Twice
> While On The Radio. This Confirms Already
> Known Additional Cases Of Jose Scott Taking
> L.S.D. More Than What Has Been Admitted.
>

> (Full Header Below Quotes)
> (Totally Searchable On Google)
>
> E.B.S. - Emergency Broadcast System
> E.A.S. - Emergency Alert System
>
> KFJC FM
> A Whole Host Of Drug Dealers And Drug Addicts
> (Spliff Skankin' Additionally), Totally Unable To
> Perform Federally (F.C.C.) Licensed Duties And
> Activities Affecting And Endangering The Lives Of
> Countless Citizens
>
> KFJC 89.7 FM -
> SHOULD LOSE THEIR F.C.C. LICENSE AND FINALLY BE
> GIVEN TO A SUITABLE ALTERNATIVE APPLICANT,
> WHERE FOOTHILL COLLEGE (KFJC) IS BEING USED TO
> PROMOTE DRUGS BY THE STAFF TO THE LISTENERS AT
> LARGE, AND A GROUPING OF DRUG DEALERS (Jose Scott,
> Steve Taiclet, Spliff Skankin (Dennis Bishop),
> WHO OPERATE AT THE RADIO STATION AT FOOTHILL
> COLLEGE.
>
> JOSE M. SCOTT -
> ADMITS TO DOING L.S.D. TWICE AT FOOTHILL COLLEGE
> KFJC 89.7 FM, AND WHILE ON THE RADIO.
> FEDERAL OFFENSE !
> TOTALLY A FEDERAL OFFENSE !
>
> ~
>
> Jose' Scott aka Hawkeye Joe
>
> (hxjx.radio.outlaw @gmail.com) wrote:
>
> # I *did* do TWO shows on LSD, the afternoon drive one,
> # the 2nd was must less emotionally draining. The
> # previous 6 - 10 pm on a Friday had me playing many
> # late 6os acid-punk stuff, and I was playing Buffalo
> # Sprinfield's "Hung Upside Down" , some New Waver
> # berated me for playing OLS stuff! I started to cry. "HY?
> # What's wrong with this?"
>
> # It was all too much that first one, the 2nd kicked ass
> # (I was "Uncle Sidney", the South Bay name we used
> # for LSD), but alas, no tape.
>
> # I always adivse new Djs to experiment, although I caution that
> # too much herb makes you slow, too much "zip" makes you
> # overly chatty, or even miore nervous, and drunk =3D sloppy ....
>
> ~ ~ ~ ~ ~ ~Header To Above Admission Post ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Exempel 3 – Phising attack

Responsable Sécurité Système d'Information <rssi@uclouvain.be> wrote
Sun, 15 Sep 2013 16:03:47 +0200:

| Dear Sir,
|
| This mail is to inform you that the "Université catholique de Louvain" has
| received phishing emails from different email addresses from all over the
| world. We replied to these phishing attack by providing fake accounts to the
| hackers.

|
| One of this account "vanessa.maes" has tried to be exploited from address
| "171.25.193.131" which belong to your network. Times below are in UTC+02.
|
| 2013-09-15T15:55:13+02:00 mmp-2-1.lan-mgt.sipr-dc.ucl.ac.be 0: [ID 800047 mail.info] Webmail
in:#011vanessa.maes@uclouvain.be at 171.25.193.131 : failed
| 2013-09-15T15:56:55+02:00 mmp-2-1.lan-mgt.sipr-dc.ucl.ac.be 0: [ID 800047 mail.info] Webmail
in:#011vanessa.maes at 171.25.193.131 : failed
|
| Please take appropriate actions ; may we ask you to keep informed about this case.

Responsable Sécurité Système d'Information <rssi@uclouvain.be> wrote
Sun, 15 Sep 2013 16:06:27 +0200:

| Dear Sir,
|
| This mail is to inform you that the "Université catholique de Louvain" has
| received phishing emails from different email addresses from all over the
| world. We replied to these phishing attack by providing fake accounts to the
| hackers.
|
| One of this account "vanessa.maes" has tried to be exploited from address
| "171.25.193.20" which belong to your network. Times below are in UTC+02.
|
| 2013-09-15T16:04:28+02:00 mmp-2-1.lan-mgt.sipr-dc.ucl.ac.be 0: [ID 800047 mail.info] Webmail
in:#011vanessa.maes@uclouvain.be at 171.25.193.20 : failed
|
| Please take appropriate actions ; may we ask you to keep informed about this case.
|
| With my best regards,
|
| X X X - PGP Key Id 0xFFFFFFF
| --
| University of Louvain - Information Service - Chief Information Security Officer
| Pythagore A.125 - Pl. des Sciences,4 bte L6.08.01 1348 Louvain-la-Neuve Belgique
| Email: X X X@uclouvain.

DFRI:s svar

Hello,

The IP address in question is a Tor exit relay, see
https://www.torproject.org/overview.html for more info about the Tor
Project.

There is little we can do to trace this matter further. As can be seen
from the overview page, the Tor network is designed to make tracing of
users impossible. The Tor network is run by some 4000 volunteers using
free software provided by the Tor Project to run Tor relays. Client
connections are routed through multiple relays. The system does not
record logs of client connections or previous hops.

To tell if a Tor exit relay is running on a given IP address, the Tor
Project provides as a service named TorDNSEL:
https://www.torproject.org/tordnsel/. Service providers
can use this tool to for example impose stricter rate limits or add a
captcha for Tor users. You can host this service yourself if you
prefer not to hand out information about your connecting clients to a
third party.

Thank you for your understanding. If you have further questions, feel
free to contact us again.

Regards

:DFRI Abuse Team

Återkoppling efter DFRI:s svar

Dear DFRI,

On 15 Sep 2013, at 16:33, :DFRI Abuse Team wrote:
> The IP address in question is a Tor exit relay, see
> https://www.torproject.org/overview.html for more info about the Tor
> Project.
Thanks for replying ! We have such a Tor exit node in our university
for research purposes.

Have a nice week-end,
XXX