一起跨国网络诈骗案件的始末

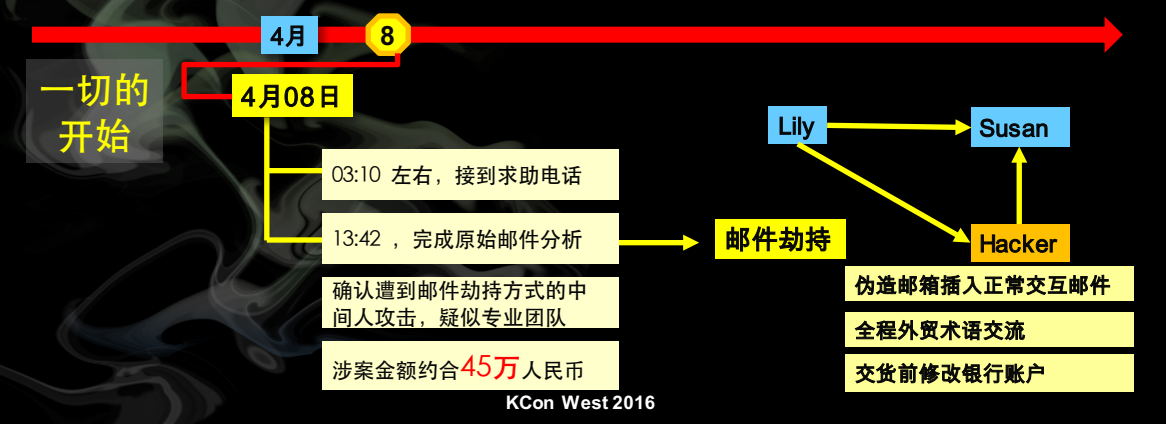
杨　哲 (Longas) | ZerOne WirelessSec Research helixus

KCon West 2016


Wi-Hack
GSM
BT
IOT
WiFi
ZigBee
SDR
GPRS
RCon West 2016
無線網路
駭客攻防
无线网络安全
攻防实战进阶

写在前面

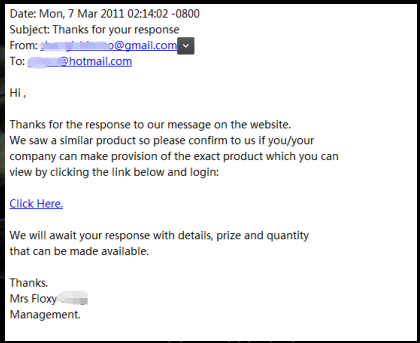
- 本案例发生在2011年，本PPT仅描述当时场景，无法代表现已升级的处理能力和技术手段
- 依照传统，隐去所有当事人姓名、职务、公司及部门真实名称
- 本案例中，涉及全部邮件正文均为无删减数据
- 本案例中，我仅代表私人身份安全顾问出现，不代表任何公司、组织及部门
- 期望本案例能对当前及未来的工作有借鉴意义


4月
8
一切的开始
4月08日
03:10 左右，接到求助电话
13:42 ，完成原始邮件分析
确认遭到邮件劫持方式的中间人攻击，疑似专业团队
涉案金额约合45万人民币
邮件劫持
Lily
Susan
Hacker
伪造邮箱插入正常交互邮件
全程外贸术语交流
交货前修改银行账户
KCon West 2016

3月 7

3月08日

02:14，美国客户**Floxy**发现货款未收到，邮件询问中方公司代表**Lily**



Date: Mon, 7 Mar 2011 02:14:02 -0800
Subject: Thanks for your response
From: [redacted]@gmail.com
To: [redacted]@hotmail.com

Hi ,

Thanks for the response to our message on the website.
We saw a similar product so please confirm to us if you/your company can make provision of the exact product which you can view by clicking the link below and login:

Click Here.

We will await your response with details, prize and quantity that can be made available.

Thanks.
Mrs Floxy [redacted]
Management.

3月 7 8

3月08日

13:48，中方公司代表**Lily**收到美国客户邮件后非常惊讶，开始询问同事

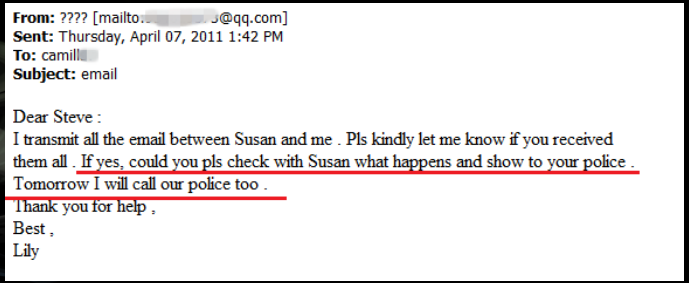
From: [redacted]@hotmail.com
To: [redacted]@gmail.com
Subject: RE: Thanks for your response
Date: Tue, 8 Mar 2011 13:48:59 +0000

Hi ,
Something seems strange , I received many customer 's reply like yours , ask me to CLICK HERE to login , then can find what you want , I tried, but never work .
If you want our products, pls send me your requirement .
we can do all the products which we already show on our list .
Best ,
Lily

3月 7 8 …… 4月 7

4月07日

13:42，中方公司代表**Lily**请求美国同事**Steve**协助检查邮件并报案



From: ???? [mailto:[redacted]@qq.com]
Sent: Thursday, April 07, 2011 1:42 PM
To: camill[redacted]
Subject: email

Dear Steve :
I transmit all the email between Susan and me . Pls kindly let me know if you received them all . If yes, could you pls check with Susan what happens and show to your police . Tomorrow I will call our police too .
Thank you for help ,
Best ,
Lily

3月 7 8 …… 4月 7 8

4月08日

01:48，美国同事**Steve**回复中方公司代表**Lily**已收到邮件打包，让英国供应商协助报案，并联系相关银行

———— Original ————

From: "camillsv";<[redacted].com>;
Date: Fri, Apr 8, 2011 01:48 AM
To: "Lily[redacted]@qq.com>;
Subject: RE: email

Lily,

We did receive the emails. Our MD in UK is contacting the police and the bank.

We'll contact you with any news.

Steve

3月 7 8 …… 4月 7 8

4月08日

04:09，美国客户方面Dave回复中方公司代表Lily，认为此次事件应为遭受黑客攻击所致，并开始联系英国BARCLAYS(巴克莱)银行，追踪货款流向

---------- Original ----------

From: "Dave [redacted]" <[redacted]>
Date: Fri, Apr 8, 2011 04:09 AM
To: "[redacted]" <[redacted]>
Cc: "camillsv" <[redacted]>, "'Susan Ardry'" <[redacted]>, "'Tom O'Keefe'" <[redacted]>, "'Mike Holding'" <[redacted]>
Subject: URGENT - Wire transfer fraud

Dear Lilly,

As we discussed today, [redacted] did not receive the funds from your company. I believe your hotmail account has been compromised and you sent the funds to a hacker in the UK. The IP addresses I investigated originated in the UK. [redacted] has no office there. [redacted], Inc. only has banking facilities in the USA. [redacted] has not bank in the UK and no association with Barclays Bank Plc. or Buga Farts.

We will assist you in any way we can to determine what happened to the funds you sent. We have a person in the UK who has contacted both Barclays Bank and the authorities in the UK to investigate where your payment went. We hope to have more information for you when we get into the office on Friday.

As the sender of the wire transfer I would recommend that you contact Barclays Bank as we have no authorization on your wire transfer or the account it was sent to.

Does your company have insurance to protect against fraud such as this?

Best regards,

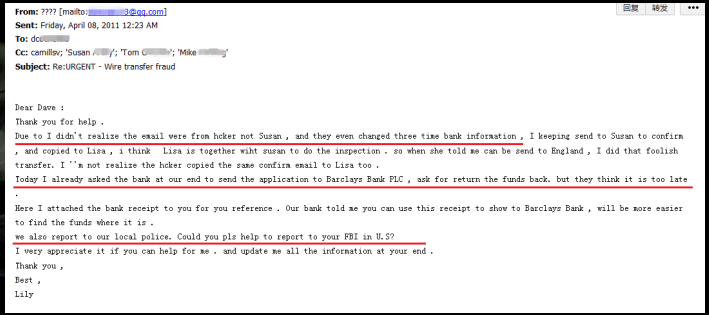
Dave

[redacted]
West Hartford, [redacted]
Phone: 860-[redacted]
Fax: 860-[redacted]

3月 7 8 …… 4月 7 8

4月08日

12:23，中方公司代表**Lily**，回复美国客户**Dave**，已通过国内银行申请向英国**BARCLAYS**(巴克莱)银行发出货款追回申请，并请求美国客户向**FBI**报案



回复 转发 •••

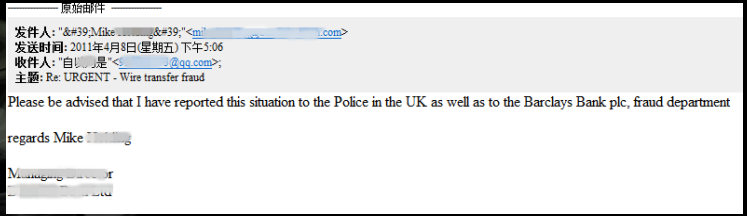
From: ???? [mailto:[redacted]3@qq.com]
Sent: Friday, April 08, 2011 12:23 AM
To: dc[redacted]
Cc: camillov; 'Susan [redacted]'; 'Tom C[redacted]'; 'Mike [redacted]'
Subject: Re:URGENT - Wire transfer fraud

Dear Dave :
Thank you for help .
Due to I didn't realize the email were from hcker not Susan , and they even changed three time bank information , I keeping send to Susan to confirm , and copied to Lisa , i think Lisa is together wiht susan to do the inspection . so when she told me can be send to England , I did that foolish transfer. I ''m not realize the hcker copied the same confirm email to Lisa too .
Today I already asked the bank at our end to send the application to Barclays Bank PLC , ask for return the funds back. but they think it is too late .
Here I attached the bank receipt to you for you reference . Our bank told me you can use this receipt to show to Barclays Bank , will be more easier to find the funds where it is .
we also report to our local police. Could you pls help to report to your FBI in U.S?
I very appreciate it if you can help for me . and update me all the information at your end .
Thank you ,
Best ,
Lily

3月 7 8 …… 4月 7 8

4月08日

17:06，英国客户同事**Mike**回复中方公司代表**Lily**，已向英国警方报案，并向英国**BARCLAYS**(巴克莱)银行发出申请



原始邮件

发件人: "'Mike'"<m[redacted].com>
发送时间: 2011年4月8日(星期五) 下午5:06
收件人: "自[redacted]是"<[redacted]@qq.com>;
主题: Re: URGENT - Wire transfer fraud

Please be advised that I have reported this situation to the Police in the UK as well as to the Barclays Bank plc, fraud department

regards Mike [redacted]

[redacted]

3月 7 8 …… 4月 7 8

4月08日

当天，受害方Lily向当地公安网监报案被拒，表示无法受理

为了协助受害方Lily，我当时向当地公安网监、北上广网安等相关人员发送技术层面分析文档，并电话寻求帮助，无果

3月 7 8 ····· 4月 7 8 9

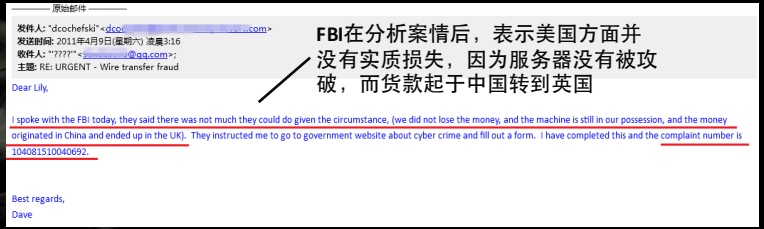
FBI WARNING

Federal Law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, or exhibition of copyrighted motion pictures (Title 17, United States Code, Sections 501 and 508). The Federal Bureau of Investigation investigates allegations of criminal copyright infringement (Title 17, United States Code, Section 506).

3月 7 8 …… 4月 7 8 9

4月09日

03:16，美国客户**Dave**回复中方公司代表**Lily**，已向**FBI**报案，立案编号：**1048081510040692**



——— 原始邮件 ———

发件人: "dccochefski"<dcc[redacted].com>
发送时间: 2011年4月9日(星期六) 凌晨3:16
收件人: "????"<[redacted]@qq.com>;
主题: RE: URGENT - Wire transfer fraud

Dear Lily,

I spoke with the FBI today, they said there was not much they could do given the circumstance, (we did not lose the money, and the machine is still in our possession, and the money originated in China and ended up in the UK). They instructed me to go to government website about cyber crime and fill out a form. I have completed this and the complaint number is 104081510040692.

Best regards,
Dave

FBI在分析案情后，表示美国方面并没有实质损失，因为服务器没有被攻破，而货款起于中国转到英国

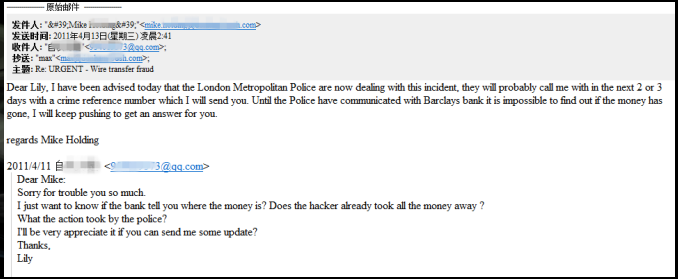
3月 7 8 …… 4月 7 8 9 11

4月11日

02:41，英国客户同事**Mike**回复中方公司代表**Lily**：目前英国警方还在处理中

连续**3**天，受害人**Lily**向当地公安经侦、网监报案先后**被拒**，都表示无法立案

注：规定金额不足**100**万，无法立案?



原始邮件

发件人: "'Mike [redacted]'"<[redacted].com>
发送时间: 2011年4月13日(星期三) 凌晨2:41
收件人: "[redacted]"<[redacted]3@qq.com>;
抄送: "max"<[redacted].com>;
主题: Re: URGENT - Wire transfer fraud

Dear Lily, I have been advised today that the London Metropolitan Police are now dealing with this incident, they will probably call me with in the next 2 or 3 days with a crime reference number which I will send you. Until the Police have communicated with Barclays bank it is impossible to find out if the money has gone, I will keep pushing to get an answer for you.

regards Mike Holding

2011/4/11 自[redacted] <[redacted]3@qq.com>

Dear Mike:
Sorry for trouble you so much.
I just want to know if the bank tell you where the money is? Does the hacker already took all the money away ?
What the action took by the police?
I'll be very appreciate it if you can send me some update?
Thanks,
Lily

3月 7 8 …… 4月 7 8 9 11 13

4月13日

22:33，英国客户同事**Mike**回复中方公司代表**Lily**：英国大都市警察厅犯罪处置部门的警官已立案，编号**5106549/11**，同时表示：

需要中国警方的官方致函，函内要说明需要协查的公司、银行等信息，否则无法继续。

当日，受害人**Lily**由于报案被拒，只能向当地市局局长求助

---------- 原始邮件 ----------

发件人："'Mike [redacted]'"<mike [redacted].com>

发送时间：2011年4月13日(星期三) 晚上10:33

收件人："9[redacted]3@qq.com";

抄送："Tatiana [redacted]"<efrei[redacted].com>;

主题：Fwd: URGENT - Wire transfer fraud

London Metropolitan Police
伦敦大都市警察厅

Dear Lily, I have now spoken with PC (Police Constable) Ablett who works at the Crime management unit at Dagenham and Barking Police station. He has recorded the crime but can take no further action until the Chinese police advise the Metropolitan police that a crime has been committed.

The Chinese Police will have established procedures for reporting crimes like this to the London Metropolitan Police and thay can tell them the crime has been recorded under Number 5106549/11 by the Dagenham and Barking police.

There is nothing more I can do, so please ask the Chinese Police to contact the Metropolitan police as soon as possible with details of the transaction, name of bank, name of Company that has suffered loss etc. so that it can be fully investigated.

regards Mike Holding

英国**BARCLAYS**(巴克莱)银行表示需要英国警方的授权，否则无法协查，建议中国警方迅速联系英国首都警署。

Barclays bank will not discuss anything to do with this matter until the UK Police advise them that some fraudulent activity has taken place. The information is with the crime management unit of Barking and Dagenham police station and they have said the crime needs to be reported to them by the Chinese Police before they can investigate. I will keep calling until I get some news.

Please ask the Chinese Police to report this crime to the metropolitan police On telephone 44 300 123 1212 and quote crime reference 44110144581 (Hampshire) regards Mike Holding

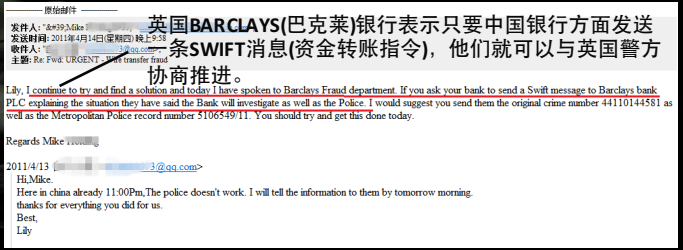
3月 7 8 …… 4月 7 8 9 11 13 14

4月14日

21:58，英国客户同事**Mike**回复中方公司代表**Lily**：英国巴克莱银行提供了一个建议。

受害人**Lily**向当地银行求助**被拒**，要求出具当地公安部门的证明

市局局长已责令立案，流程为由地区上报市局，再提交省厅，最后提交公安部


原始邮件

发件人：'Mike
发送时间：2011年4月14日(星期四) 晚上9:58
收件人：
主题：Re: Fwd: URGENT - wire transfer fraud

Lily, I continue to try and find a solution and today I have spoken to Barclays Fraud department. If you ask your bank to send a Swift message to Barclays bank PLC explaining the situation they have said the Bank will investigate as well as the Police. I would suggest you send them the original crime number 44110144581 as well as the Metropolitan Police record number 5106549711. You should try and get this done today.

Regards Mike

2011/4/13 3@qq.com>
Hi,Mike.
Here in china already 11:00Pm,The police doesn't work. I will tell the information to them by tomorrow morning.
thanks for everything you did for us.
Best,
Lily

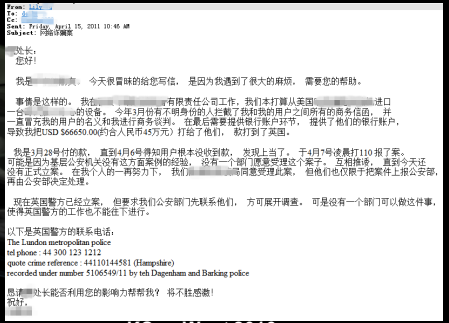
英国**BARCLAYS**(巴克莱)银行表示只要中国银行方面发送一条**SWIFT**消息(资金转账指令)，他们就可以与英国警方协商推进。

3月 7 8 …… 4月 7 8 9 11 13 14 15

4月15日

鉴于当地公安机关没有相关经验，报案流程缓慢，而国外银行一直在催促材料。

10:45，受害人**Lily**尝试向中国国家商务部某部门负责人邮件求助，寻求加快推动处理


From: Lily
To:
Cc:
Sent: Friday, April 15, 2011 10:46 AM
Subject: 问题调查

处长，
您好！

我是 ，今天很冒昧的给您写信，是因为我遇到了很大的麻烦，需要您的帮助。

事情是这样的，我在 有限责任公司工作，我们本打算从英国 进口一台 的设备。今年3月份有不明身份的人拦截了我和我的用户之间所有的商务信函，并一直冒充我的用户的名义和我进行商务谈判。在最后需要提供银行账户环节，提供了他们的银行账户，导致我把USD $66650.00的合人民币45万元）打给了他们，款打到了英国。

我是3月28号付的款，直到4月6号得知用户根本没收到款，发现上当了，于4月7号凌晨打110报了案。可能是因为英国公安机关没有这方面案例的经验，没有一个部门愿意受理这个案子，互相推诿，直到今天还没有正式立案。在我个人的一再努力下，我们 同意受理此案，但他们也仅限于把案件上报公安部，再由公安部决定处理。

现在英国警方已经立案，但要求我们公安部门先联系他们，方可展开调查。可是没有一个部门可以做这件事，使得英国警方的工作也不能往下进行。

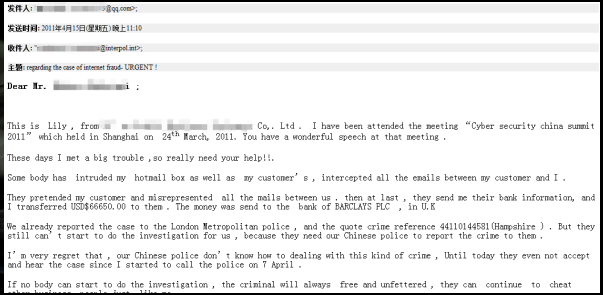
以下是英国警方的联系电话：
The Lundon metropolitan police
tel phone : 44 300 123 1212
quote crime reference : 4411014455\1 (Hampshire)
recorded under number 5106549/11 by teh.Dagenham and Barking police

恳请 处长能否利用您的影响力帮帮我？ 将不胜感激！
祝好，

3月 7 8 …… 4月 7 8 9 11 13 14 15

4月15日

11:10，受害人Lily尝试向国际刑警亚太区某部门负责人求助，寻求能够加快推动国际间事务处理的办法



发件人： [redacted]>@qq.com>;

发送时间： 2011年4月15日(星期五) 晚上11:10

收件人： "[redacted]@interpol.int>;

主题： regarding the case of internet fraud- URGENT !

Dear Mr. [redacted] ;

This is Lily , from [redacted] Co,. Ltd . I have been attended the meeting "Cyber security china summit 2011" which held in Shanghai on 24th March, 2011. You have a wonderful speech at that meeting .

These days I met a big trouble ,so really need your help!!.

Some body has intruded my hotmail box as well as my customer's , intercepted all the emails between my customer and I .

They pretended my customer and misrepresented all the mails between us . then at last , they send me their bank information, and I transferred USD$66650.00 to them . The money was send to the bank of BARCLAYS PLC , in U.K

We already reported the case to the London Metropolitan police , and the quote crime reference 44110144581(Hampshire) . But they still can't start to do the investigation for us , because they need our Chinese police to report the crime to them .

I'm very regret that , our Chinese police don't know how to dealing with this kind of crime , Until today they even not accept and hear the case since I started to call the police on 7 April .

If no body can start to do the investigation , the criminal will always free and unfettered , they can continue to cheat

3月 7 8 …… 4月 7 8 9 11 13 14 15 16

4月16日

00:28，中国国家商务部某部门负责人回复受害人**Lily**：建议通过省公安厅联系英国警方，并提供伦敦大使馆的联系方式

发件人： "[redacted]@mofcom.gov.cn>;
发送时间: 2011年4月16日(星期六) 凌晨0:28
收件人: "Li[redacted]@qq.com>;
抄送: "[redacted]
主题: Re: 网络诈骗案

[redacted].

你好！

非常同情你的遭遇，对于此类事件我也没有什么经验，我个人认为你可以要求你们省公安厅联系英国警方，我也可以告诉你我们伦敦大使馆的联系方式，看看他们能不能帮上忙？

电话: 0044 20 7087 4949
传真: 0044 20 7706 2777
地址： 16， Lancaster Gate, London, UK
邮编： W2 3LH

[redacted]

3月 7 8 …… 4月 7 8 9 11 13 14 15 16 18

4月18日

09:28，美国客户同事邮件受害人**Lily**:

要求尽快提供中国警方提交英国警方的协查报告，以及中国方面银行的退款申请函，这样英国警方就能展开工作！

截至当日，受害人**Lily**去当地市公安局查询，得知仍未收到地区上报的案件材料

发件人: "jenny";<[redacted]n.cn>;
发送时间: 2011年4月18日(星期一) 上午9:28
收件人: "Lily [redacted]@qq.com>
主题: 答复: 转发: 回复: Fwd: URGENT - Wire transfer fraud

Lily, 两件事需要尽快：1.[redacted]警察发给英国警察的报告。2. 银行要求退款的信函。这样英国警方就可以开展工作，就有希望破案。

让我们一起努力，尽快追回损失。

Jenny 林

3月 7 8 …… 4月 7 8 9 11 13 14 15 16 18

4月18日

23:11，英国客户同事**Mike**通知中方公司代表**Lily**：

英国巴克莱银行账户出现异常行为，货款已被快速转走，银行已经知会英国警方！但由于始终没有收到中国方面的材料，他们无能为力

截至当日，受害人**Lily**去当地省公安厅查询，得知仍未收到市局上报的案件材料

原始邮件

发件人： "'Mike [redacted]>;
发送时间： 2011年4月18日(星期一) 晚上11:11
收件人： "[redacted]@qq.com>;
主题： Fwd: 回复： Fwd: URGENT - Wire transfer fraud

Lily-

Please find below a copy of the message I received today from the Metropolitan Police. They have said that your bank must contact Barclays fraud office and report the loss. Your bank should refer to the police record number 5106549/11 as well as details of the victim, i.e. your companies name , bank account details etc. Once the bank receives this notification from your bank they will communicate with Police who will then investigates transaction. I feel we have now made some progress but it is important that your bank contact Barclays bank as soon as possible.You can call 44 1604 252 073 (Contact is Stephanie).

Update 18 April 2011:

货款被快速转走，追回希望渺茫，估计你所在公司会走法律渠道向个人索要赔偿

Lily-

I have spoken with Barclays bank fraud line again to day and they have confirmed which account the money went into and will now show it as 'suspicious activity'. They are not very hopeful that we will be able to recover the money but they are now reporting it to the Police as they can see the transaction.

The money was taken out of the account very quickly but as above they are not very hopeful of getting it back, so your company would need to take the person to court for compensation. If your bank contact barclays that may speed things up but I now have the Bank and the Police talking to each other which is good. Do your company have afirm of solicitors in China and if so do they have contact with a UK or USA firm of solicitors. Thank you for the letter of authorisation and the account details I will pass them on to the Police and the bank as soon as I am able.

Regards Mike Holding

3月 7 8 …… 4月 7 8 9 11 13 14 15 16 18 19

4月19日

21:34，国际刑警亚太区某部门负责人回复受害人**Lily**：

建议联系中国方面的国际刑警部门

建议继续跟进当地警方

截至当日，受害人**Lily**去当地省公安厅查询，得知仍未收到市局上报的案件材料

发件人: "N[redacted]"<[redacted]@INTERPOL.INT>;
发送时间: 2011年4月19日(星期二) 晚上9:34
收件人: "Lily[redacted]@qq.com>;
主题: RE: 转发：regarding the case of internet fraud- URGENT !

Dear [redacted]

Please take a look at the advice from our Chinese seconded officer from the Ministry of Public Security of China.

I think that you can count on the local police authority regarding your case.

I hope that your case will be resolved soon.

Best Regards,

[redacted]
Director
Information Systems and Technology Directorate

O.I.P.C. -INTERPOL
TEL: (33)4 72 44 70 40
Email: n.nakatani@interpol.int

受害人Lily最终未收到当地公安部门的任何反馈，数次电话及上门询问无果，无奈放弃

英国警方最终也没有得到任何中国方面的警方资料，只能将案件搁置，直至有效期结束

货款最终被转移数次后，消失在非洲……

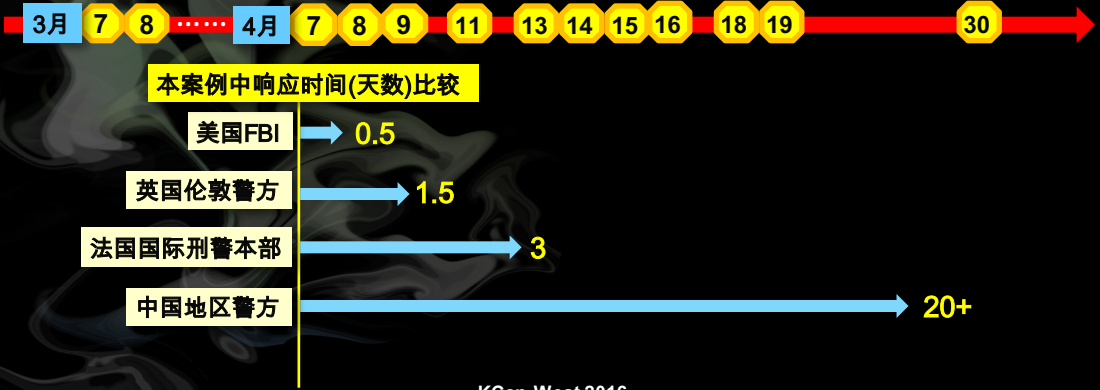
不是每个故事都有美好结局

前后一个月，受害人Lily几近奔溃

由于个人疏忽导致公司重大损失，受害人Lily面临被所在公司起诉：
当事人被公司怀疑私吞钱款，公司停发工资，并要求当事人返还钱款

最终达成协议：

1）继续为公司做销售工作
2）无月薪、奖金，无任何福利
3）完成45万损失对应销售额后可离开


3月
7
8
……
4月
7
8
9
11
13
14
15
16
18
19
30
本案例中响应时间(天数)比较
美国FBI
0.5
英国伦敦警方
1.5
法国国际刑警本部
3
中国地区警方
20+

五年过去了，现在的我们是不是能做得更好?

杨 哲
(Longas)
ZerOne无线安全研究组织

ZerOne
WirelessSec Research

KCon West 2016