一起跨国网络诈骗案件的始末

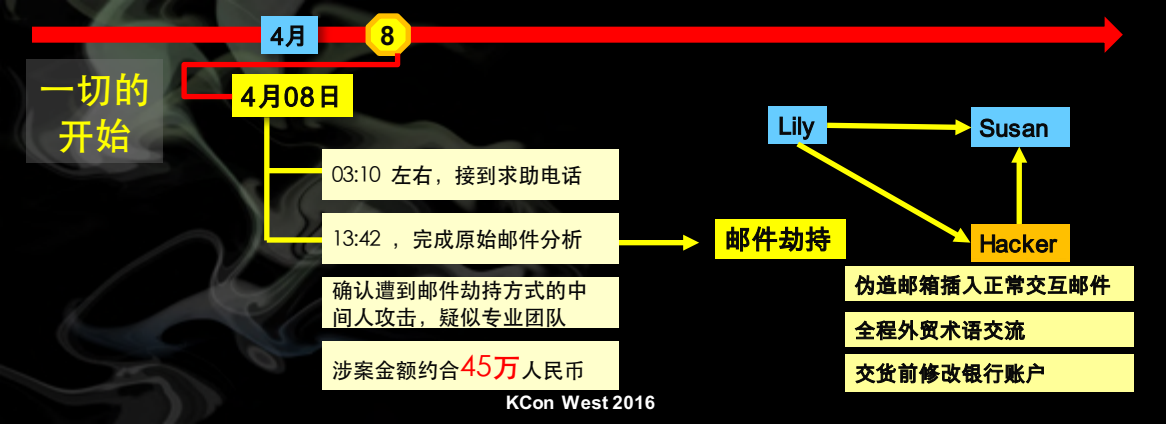
杨　哲 (Longas) | ZerOne WirelessSec Research helixus

KCon West 2016


Wi-Hack
無線網路
駭客攻防
GSM
BT
IOT
WiFi
ZigBee
SDR
GPRS
RCon West 2016

写在前面

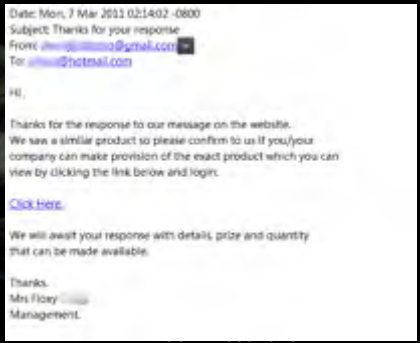
- 本案例发生在2011年，本PPT仅描述当时场景，无法代表现已升级的处理能力和技术手段
- 依照传统，隐去所有当事人姓名、职务、公司及部门真实名称
- 本案例中，涉及全部邮件正文均为无删减数据
- 本案例中，我仅代表私人身份安全顾问出现，不代表任何公司、组织及部门
- 期望本案例能对当前及未来的工作有借鉴意义


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, price 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

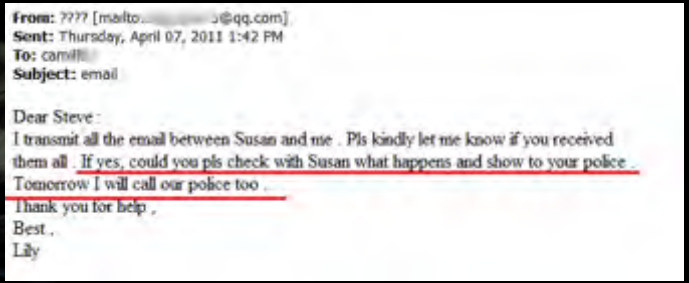

From: @hotmail.com
To: @gmail.com
Subject: RE: Thanks for your response
Date: Tue, 8 Mar 2011 13:48:59 +0000

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: "camillv";<[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.

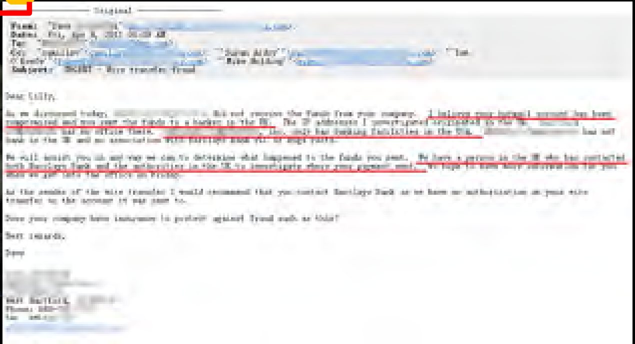
We'll contact you with any news.

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



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


From: [redacted]
Sent: Friday, April 08, 2011 12:23 AM
To: [redacted]
CC: [redacted]
Subject: RE:URGENT - Wire transfer Fraud

Dear Dave :
Thank you for help ;
Due to I didn't realize the email were from hker not Suzan , and they even changed three time bank information , I keeping send to Suzan to confirm , and copied to Lisa , u think . Lisa is together with wangs to do the inspection , so when she told me can be send to England , I did that foolish. transfer. I 'm not realize the hker copied the same confirm email to Lisa too .
Today I already asked the bank at once and to cancel 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 . the 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 plz help to report to your FBI as 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

KCon West 2016

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:

发送时间:

收件人:

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

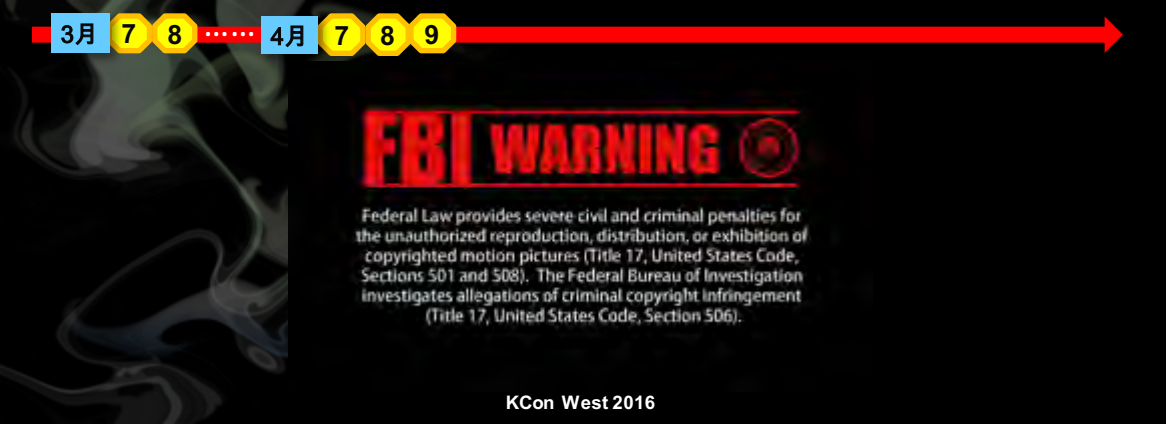
3月 7 8 …… 4月 7 8

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

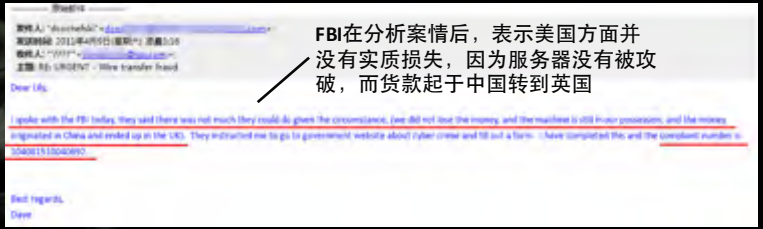
3月 7 8 ····· 4月 7 8 9


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**



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 1048081510040692

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?

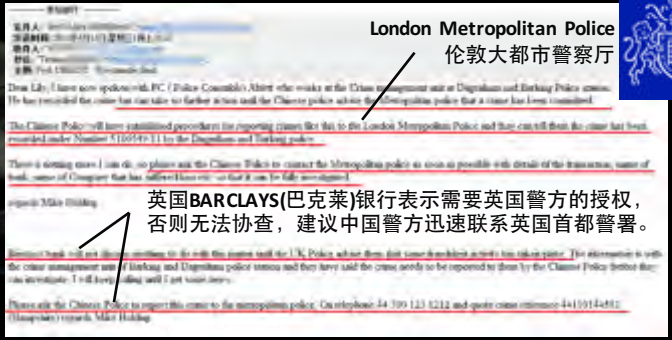
3月 7 8 …… 4月 7 8 9 11 13

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



Dear Lily, I have now spoken with PC (Police Constable) Abbitt 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 they 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

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 trying 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 4410314e911

Dagenham regards Mike Holding

London Metropolitan Police
伦敦大都市警察厅

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。

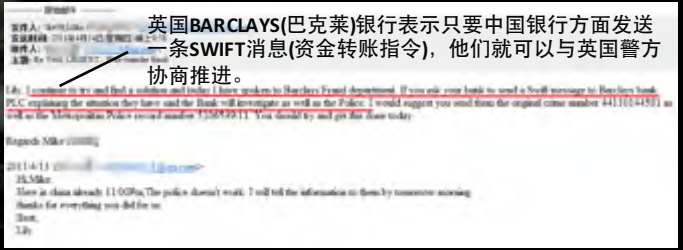
3月 7 8 …… 4月 7 8 9 11 13 14

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



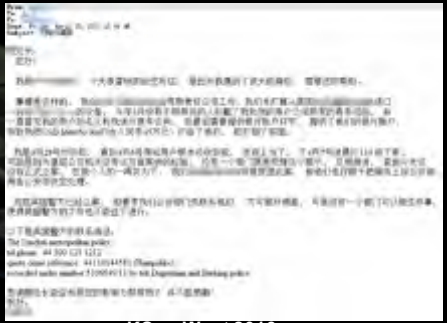
英国**BARCLAYS**(巴克莱)银行表示只要中国银行方面发送条**SWIFT**消息(资金转账指令)，他们就可以与英国警方协商推进。

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



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

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

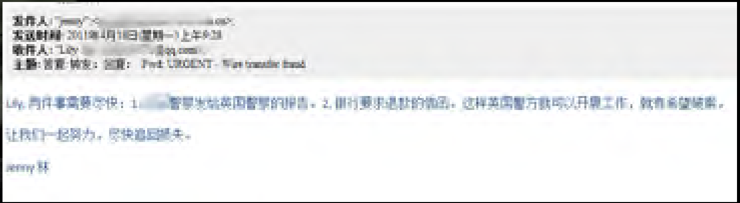
3月 7 8 …… 4月 7 8 9 11 13 14 15 16 18

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



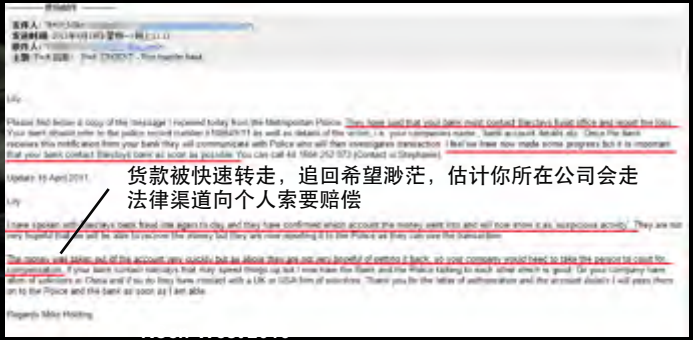
3月 7 8 …… 4月 7 8 9 11 13 14 15 16 18

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



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 local office and report the loss. Your bank should refer to the police record number 1108/4/7/11 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 investigate transaction that your bank contact Barclays bank as soon as possible. You can call 44 1604 252 973 (Contact is Stephanie)

I feel we have now made some progress but it is important

Update: 19 April 2017

Lily

I have spoken with Barclays bank fraud one 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 allot 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 Hosking

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

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

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

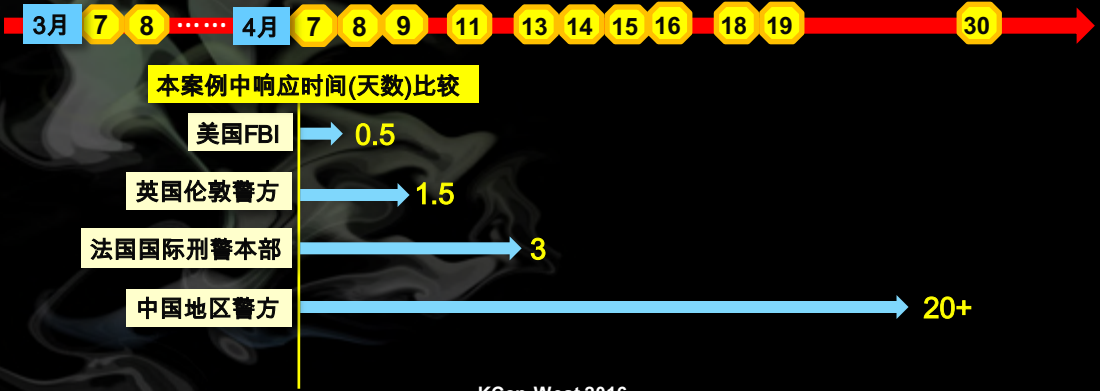
货款最终被转移数次后，消失在非洲……

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

KCon West 2016