

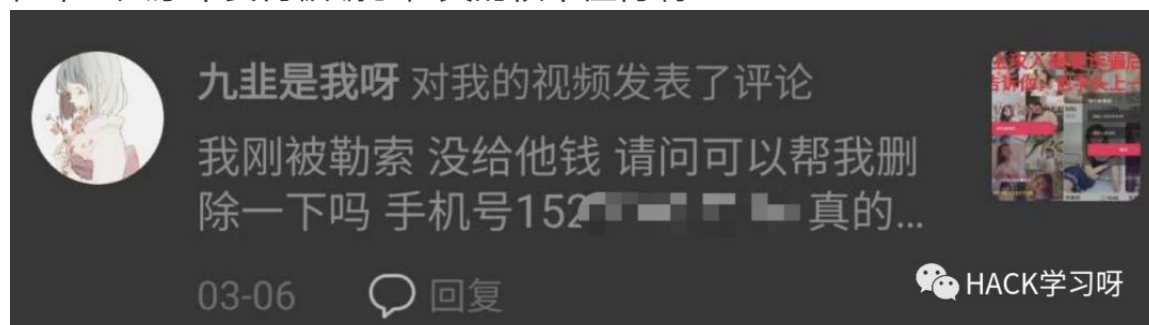
当粉丝遇到裸聊诈骗，我们花了1天时间控制了诈骗犯的电脑

原创 HACK学习 HACK学习呀

2020-03-08原文

0X01

3月6日，突然又一位B站粉丝找我，说自己被骗，最近裸聊诈骗高发，希望大家不要再被骗了，真的很不值得啊！



正好快周末了，我就帮他看了以下这个App平台，和以前遇到的一样，也是这套模板和话术，但是这一次，我们拿到了shell，并把诈骗分子的机器控制了下来

0X02

我与被骗者粉丝的聊天对话

周五 17:24

我是非兔,我刚被勒索 没给他钱 请问可以帮我删除一下吗 手机号152 真的害怕。

以上是打招呼的内容

你已添加了韭兔兔，现在可以开始聊天了。

• 8"

• 8"

•) 7"



别会群发到你的手机上。这些人他们也不可能想着你这个网友不管。说让你小偷偷我也不想打你家人。行不行一句话，不管每天定好手机费发给你几万几十万让你的通讯录看着你的手机过日子吧。



受害人与诈骗分子的聊天对话



解除关系



加为好友



兄弟要不要解决 我也就图点小钱,你买个面子 2000块帮你删除视频、钱到位我跟你开视频摄像头对着电脑上帮你永久删除你裸聊的视频。如果你不想解决视频会群发到你的通讯录.这你家人他们总不可能放着你这个视频不管,这么点小钱我也不想打扰你家人。行不行一句话,不给每天设定好系统群发轰炸几百几千遍让你的通讯录看着你打飞机过日子吧

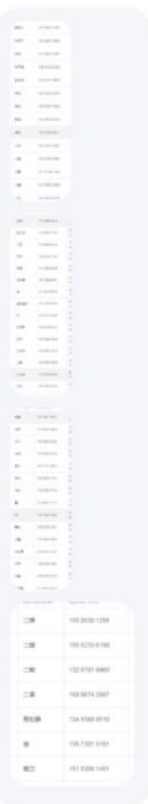


204511	150 1810 1810
204577	150 1817 1810
204588	150 1810 1810
204594	150 1810 1810
204602	150 1817 1810
204610	150 1817 1810
204618	150 1810 1810
204626	150 1810 1810
204634	150 1810 1810
204642	150 1810 1810
204650	150 1810 1810
204658	150 1810 1810
204666	150 1810 1810
204674	150 1810 1810
204682	150 1810 1810
204690	150 1810 1810
204698	150 1810 1810
204706	150 1810 1810
204714	150 1810 1810
204722	150 1810 1810
204730	150 1810 1810
204738	150 1810 1810
204746	150 1810 1810
204754	150 1810 1810
204762	150 1810 1810
204770	150 1810 1810
204778	150 1810 1810
204786	150 1810 1810
204794	150 1810 1810
204802	150 1810 1810
204810	150 1810 1810
204818	150 1810 1810
204826	150 1810 1810
204834	150 1810 1810
204842	150 1810 1810
204850	150 1810 1810
204858	150 1810 1810
204866	150 1810 1810
204874	150 1810 1810
204882	150 1810 1810
204890	150 1810 1810
204898	150 1810 1810
204906	150 1810 1810
204914	150 1810 1810
204922	150 1810 1810
204930	150 1810 1810
204938	150 1810 1810
204946	150 1810 1810
204954	150 1810 1810
204962	150 1810 1810
204970	150 1810 1810
204978	150 1810 1810
204986	150 1810 1810
204994	150 1810 1810
205002	150 1810 1810
205010	150 1810 1810
205018	150 1810 1810
205026	150 1810 1810
205034	150 1810 1810
205042	150 1810 1810
205050	150 1810 1810
205058	150 1810 1810
205066	150 1810 1810
205074	150 1810 1810
205082	150 1810 1810
205090	150 1810 1810
205098	150 1810 1810
205106	150 1810 1810
205114	150 1810 1810
205122	150 1810 1810
205130	150 1810 1810
205138	150 1810 1810
205146	150 1810 1810
205154	150 1810 1810
205162	150 1810 1810
205170	150 1810 1810
205178	150 1810 1810
205186	150 1810 1810
205194	150 1810 1810
205202	150 1810 1810
205210	150 1810 1810
205218	150 1810 1810
205226	150 1810 1810
205234	150 1810 1810
205242	150 1810 1810
205250	150 1810 1810
205258	150 1810 1810
205266	150 1810 1810
205274	150 1810 1810
205282	150 1810 1810
205290	150 1810 1810
205298	150 1810 1810
205306	150 1810 1810
205314	150 1810 1810
205322	150 1810 1810
205330	150 1810 1810
205338	150 1810 1810
205346	150 1810 1810
205354	150 1810 1810
205362	150 1810 1810
205370	150 1810 1810
205378	150 1810 1810
205386	150 1810 1810
205394	150 1810 1810
205402	150 1810 1810
205410	150 1810 1810
205418	150 1810 1810
205426	150 1810 1810
205434	150 1810 1810
205442	150 1810 1810
205450	150 1810 1810
205458	150 1810 1810
205466	150 1810 1810
205474	150 1810 1810
205482	150 1810 1810
205490	150 1810 1810
205498	150 1810 1810
205506	150 1810 1810
205514	150 1810 1810
205522	150 1810 1810
205530	150 1810 1810
205538	150 1810 1810
205546	150 1810 1810
205554	150 1810 1810
205562	150 1810 1810
205570	150 1810 1810
205578	150 1810 1810
205586	150 1810 1810
205594	150 1810 1810
205602	150 1810 1810
205610	150 1810 1810
205618	150 1810 1810
205626	150 1810 1810
205634	150 1810 1810
205642	150 1810 1810
205650	150 1810 1810
205658	150 1810 1810
205666	150 1810 1810
205674	150 1810 1810
205682	150 1810 1810
205690	150 1810 1810
205698	150 1810 1810
205706	150 1810 1810
205714	150 1810 1810
205722	150 1810 1810
205730	150 1810 1810
205738	150 1810 1810
205746	150 1810 1810
205754	150 1810 1810
205762	150 1810 1810
205770	150 1810 1810
205778	150 1810 1810
205786	150 1810 1810
205794	150 1810 1810
205802	150 1810 1810
205810	150 1810 1810
205818	150 1810 1810
205826	150 1810 1810
205834	150 1810 1810
205842	150 1810 1810
205850	150 1810 1810
205858	150 1810 1810
205866	150 1810 1810
205874	150 1810 1810
205882	150 1810 1810
205890	150 1810 1810
205898	150 1810 1810
205906	150 1810 1810
205914	150 1810 1810
205922	150 1810 1810
205930	150 1810 1810
205938	150 1810 1810
205946	150 1810 1810
205954	150 1810 1810
205962	150 1810 1810
205970	150 1810 1810
205978	150 1810 1810
205986	150 1810 1810
205994	150 1810 1810
206002	150 1810 1810
206010	150 1810 1810
206018	150 1810 1810
206026	150 1810 1810
206034	150 1810 1810
206042	150 1810 1810
206050	150 1810 1810
206058	150 1810 1810
206066	150 1810 1810
206074	150 1810 1810
206082	150 1810 1810
206090	150 1810 1810
206098	150 1810 1810
206106	150 1810 1810
206114	150 1810 1810
206122	150 1810 1810
206130	150 1810 1810
206138	150 1810 1810
206146	150 1810 1810
206154	150 1810 1810
206162	150 1810 1810
206170	150 1810 1810
206178	150 1810 1810
206186	150 1810 1810
206194	150 1810 1810
206202	150 1810 1810
206210	150 1810 1810
206218	150 1810 1810
206226	150 1810 1810
206234	150 1810 1810
206242	150 1810 1810
206250	150 1810 1810
206258	150 1810 1810
206266	150 1810 1810
206274	150 1810 1810
206282	150 1810 1810
206290	150 1810 1810
206298	150 1810 1810
206306	150 1810 1810
206314	150 1810 1810
206322	150 1810 1810
206330	150 1810 1810
206338	150 1810 1810
206346	150 1810 1810
206354	150 1810 1810
206362	150 1810 1810
206370	150 1810 1810
206378	150 1810 1810
206386	150 1810 1810
206394	150 1810 1810
206402	150 1810 1810
206410	150 1810 1810
206418	150 1810 1810
206426	150 1810 1810
206434	150 1810 1810
206442	150 1810 1810
206450	150 1810 1810
206458	150 1810 1810
206466	150 1810 1810
206474	150 1810 1810
206482	150 1810 1810
206490	150 1810 1810
206498	150 1810 1810
206506	150 1810 1810
206514	150 1810 1810
206522	150 1810 1810
206530	150 1810 1810
206538	150 1810 1810
206546	150 1810 1810
206554	150 1810 1810
206562	150 1810 1810
206570	150 1810 1810
206578	150 1810 1810
206586	150 1810 1810
206594	150 1810 1810
206602	150 1810 1810
206610	150 1810 1810
206618	150 1810 1810
206626	150 1810 1810
206634	150 1810 1810
206642	150 1810 1810
206650	150 1810 1810
206658	150 1810 1810
206666	150 1810 1810
206674	150 1810 1810
206682	150 1810 1810
206690	150 1810 1810
206698	150 1810 1810
206706	150 1810 1810
206714	150 1810 1810
206722	150 1810 1810
206730	150 1810 1810
206738	150 1810 1810
206746	150 1810 1810
206754	150 1810 1810
206762	150 1810 1810
206770	150 1810 1810
206778	150 1810 1810
206786	150 1810 1810
206794	150 1810 1810
206802	150 1810 1810
206810	150 1810 1810
206818	150 1810 1810
206826	150 1810 1810
206834	150 1810 1810
206842	150 1810 1810
206850	150 1810 1810
206858	150 1810 1810
206866	150 1810 1810
206874	150 1810 1810
206882	150 1810 1810
206890	150 1810 1810
206898	150 1810 1810
206906	150 1810 1810
206914	150 1810 1810
206922	150 1810 1810
206930	150 1810 1810
206938	150 1810 1810
206946	150 1810 1810
206954	150 1810 1810
206962	150 1810 1810
206970	150 1810 1810
206978	150 1810 1810
206986	150 1810 1810
206994	150 1810 1810
207002	150 1810 1810
207010	150 1810 1810
207018	150 1810 1810
207026	150 1810 1810
207034	150 1810 1810
207042	150 1810 1810
207050	150 1810 1810
207058	150 1810 1810
207066	150 1810 1810
207074	150 1810 1810
207082	150 1810 1810
207090	150 1810 1810
207098	150 1810 1810
207106	150 1810 1810
207114	150 1810 1810
207122	150 1810 1810
207130	150 1810 1810
207138	150 1810 1810
207146	150 1810 1810
207154	150 1810 1810
207162	150 1810 1810
207170	150 1810 1810
207178	150 1810 1810
207186	150 1810 1810
207194	150 1810 1810
207202	150 1810 1810
207210	150 1810 1810
207218	150 1810 1810
207226	150 1810 1810
207234	150 1810 1810
207242	150 1810 1810
207250	150 1810 1810
207258	150 1810 1810
207266	150 1810 1810
207274	150 1810 1810
207282	150 1810 1810
207290	150 1810 1810
207298	150 1810 1810
207306	150 1810 1810
207314	150 1810 1810
207322	150 1810 1810
207330	150 1810 1810
207338	150 1810 1810
207346	150 1810 1810
207354	150 1810 1810
207362	150 1810 1810
207370	150 1810 1810
207378	150 1810 1810
207386	150 1810 1810
207394	150 1810 1810
207402	150 1810 1810
207410	150 1810 1810
207418	150 1810 1810
207426	150 1810 1810
207434	150 1810 1810
207442	150 1810 1810
207450	150 1810 1810
207458	150 1810 1810
207466	150 1810 1810
207474	150 1810 1810
207482	150 1810 1810
207490	150 1810 1810
207498	150 1810 1810
207506	150 1810 1810
207514	150 1810 1810
207522	150 1810 1810
207530	150 1810 1810
207538	150 1810 1810
207546	150 1810 1810
207554	150 1810 1810
207562	150 1810 1810
207	

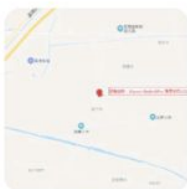
开始威胁勒索



兄弟要不要解决 我也就图点小钱，你买个面子 2000块帮你删除视频、钱到位我跟你开视频摄像头对着电脑上帮你永久删除你裸聊的视频。如果你不想解决视频会群发到你的通讯录。这你家人他们总不可能放着你这个视频不管，这么点小钱我也不想打扰你家人。行不行一句话，不给每天设定好系统群发轰炸几百几千遍让你的通讯录看着你打飞机过日子吧



不处理吗？难道你要我给你的通讯录群发轰炸？



你想多了 这是HACK的卡



再帮你当个网红？

HACK学习呀

我与受害人的聊天对话

晚上我看看吧



你把 app 二维码发给我



谢谢哥



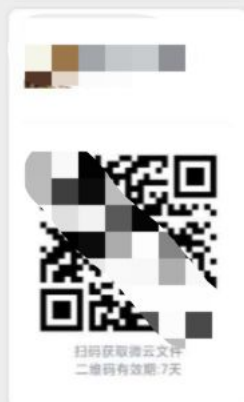
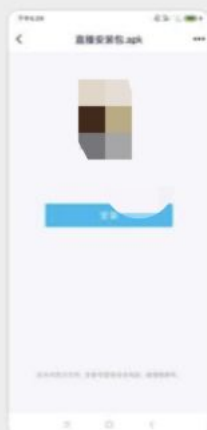
没有 他只给我一个软件



对啊



软件发给我



抓包获得域名，然后找到了后台，又一次凭借弱口令进了后台，运气真好

周五 21:45

软件邀请码是什么



邀请 是 688805

3559	311025
2	243803
0	0
0	0



进来了



手机号多少



谢谢 15 6

手机号	邀请码	最后登录时间	最后登录IP地址	最后登录位置	操作
1540			16	中国山东菏泽	在线定位 下载通讯录 清空短信



这个人吗



对



对



已删除



嗯



谢谢哥



我是不是安全了

客气了



非常感谢

不明确对方是不是有备份



up 主太好了



嗯

虽然进来诈骗管理后台，删除了受害人的信息，但是刚好趁着周末有空，顺便看看能不能拿shell，再钓个鱼看看，这次运气不错，后台可以上传Getshell

如何利用XSS钓鱼，可以参考阅读：

记一次BC站实战渗透 | 从XSS到主机上线



















0X03

顺利拿到shell，然后利用XSS钓鱼成功钓上了诈骗分子的电脑，让我们看看他电脑上到底有什么。

				5	192.168.0.100	Administrator *				357	Bid: 6806 Arch: x64 Ver: 6.1	2060
				100	192.168.0.101	Administrator *				528	Bid: 90645 Arch: x64 Ver: 6.1	66312

目标上线，目标机器上有QQ电脑管家，还好我的马免杀，美滋滋

我们从目标机器上下载回来的一些文件

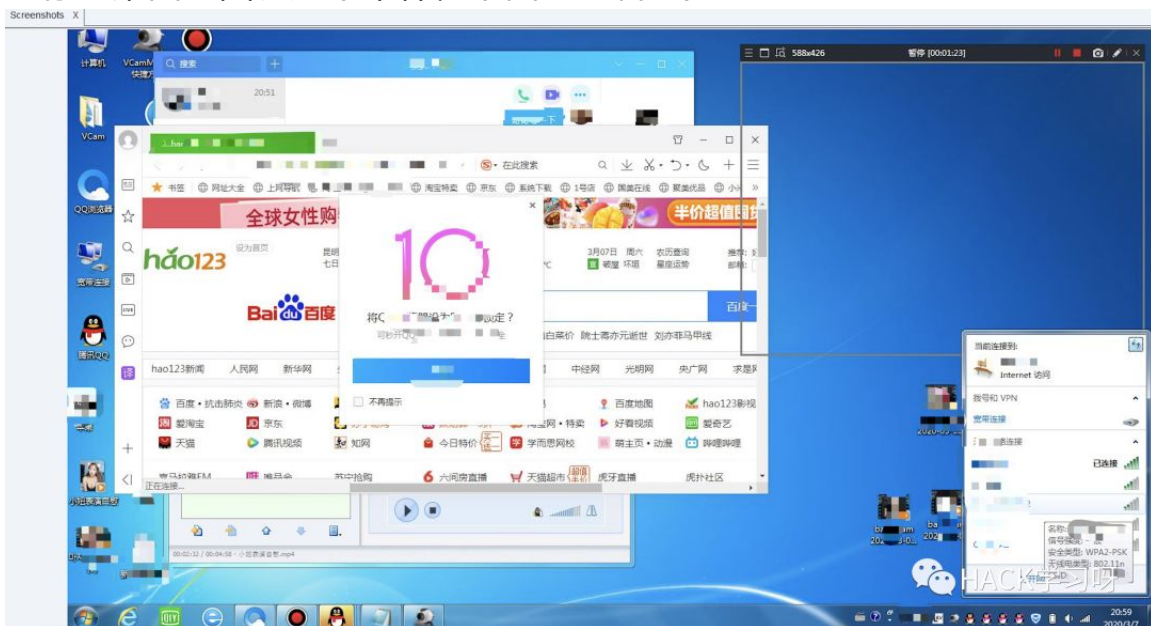
Event Log X		Screenshots X		Downloads X								
host						name	path	size	date			
192.16		101				最新话术.txt	c:\users\Administrator\Desktop\	2kb	03/07 21:07:			
192.16		101				小姑表演自慰.mp4	c:\users\Administrator\Desktop\	27mb	03/07 21:11:			
192.16		101				新建文本文档.txt	c:\users\Administrator\Desktop\	13b	03/07 21:11:			
192.16		101				安卓.png	c:\users\Administrator\Desktop\	3kb	03/07 21:11:			
192.16		101				苹果.png	c:\users\Administrator\Desktop\	9kb	03/07 21:12:			
192.16		101				DEDA5468544E425D709346A13D58D012(1).jpg	c:\users\Administrator\Desktop\	125kb	03/07 21:13:			
192.16		101				C48BABC649BCB836C415DA986495439F.png	c:\users\Administrator\Desktop\	227kb	03/07 21:13:			
192.16		101				A960FA17121A5B46037F6E96FA7315D2.png	c:\users\Administrator\Desktop\	241kb	03/07 21:13:			
192.16		101				656470910EF093CA8974800FAEE3A4F.png	c:\users\Administrator\Desktop\	235kb	03/07 21:13:			
192.16		101				5C7BC12F22C49DBCF061A89E5E2ACDF.jpg	c:\users\Administrator\Desktop\	39kb	03/07 21:13:			
192.16		101				47D93F51CAE0CF9F51E0157DDCAE8BF3.png	c:\users\Administrator\Desktop\	236kb	03/07 21:13:			
192.16		101				2345截图20200302005317.png	C:\Users\Administrator\Documents\2345截图\	681kb	03/07 21:16:			
192.16		101				bandicam 2020-03-06 21-02-19-553.avi	C:\Users\Administrator\Desktop\	6mb	03/07 21:19:			
192.16		100				Msg3.0.db	C:\Users\Administrator\Documents\Tencent Files\0...	1mb	03/07 21:26:			
192.16		100				Msg3.0.db	C:\Users\Administrator\Documents\Tencent Files\1...	2mb	03/07 21:26:			
192.16		100				Msg3.0.db	C:\Users\Administrator\Documents\Tencent Files\14...	3mb	03/07 21:37:			
192.16		100				Msg3.0.db	C:\Users\Administrator\Documents\Tencent Files\17...	3mb	03/07 21:40:			
192.16		100				Msg3.0.db	C:\Users\Administrator\Documents\Tencent Files\11...	3mb	03/07 21:44:			

诈骗分子准备的QQ号：

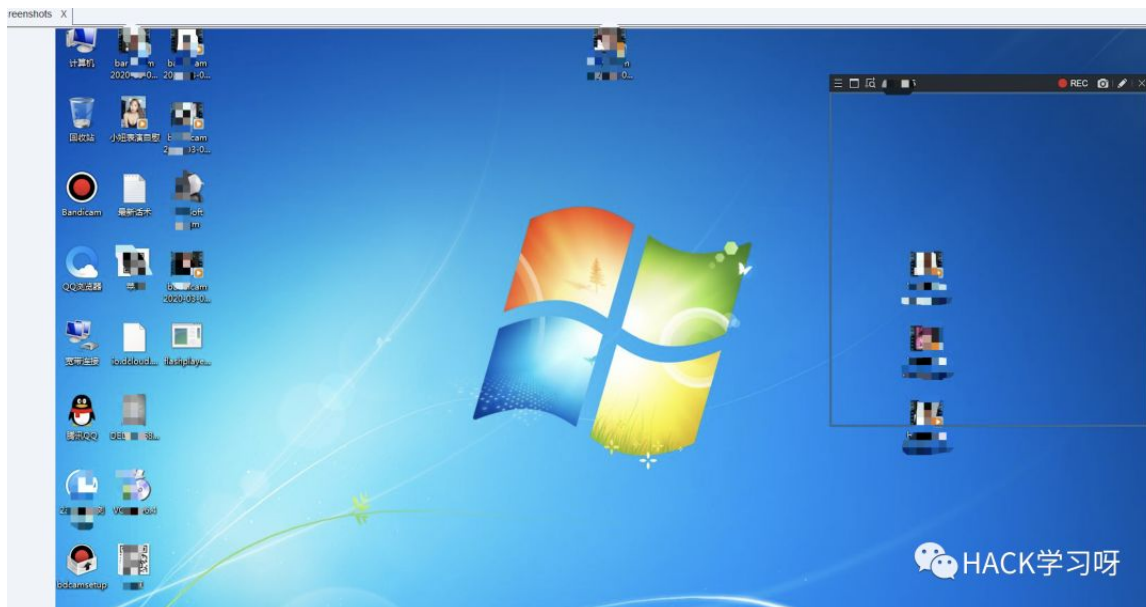
C:\Users\Administrator\Documents\Tencent Files\			
D -	Name	Size	Modified
	345		03/07/2020 18:42
	543		03/06/2020 21:13
	595	5	03/05/2020 16:07
	05	15	03/03/2020 20:02
	145	65	03/02/2020 16:06
	12	65	03/02/2020 16:10
	5	115	03/02/2020 15:02
	56	35	03/03/2020 19:06
	43	15	03/02/2020 01:20
	676	5	03/01/2020 19:10
	1148	7	03/02/2020 02:40
	877	0	03/04/2020 23:07
	996	15	03/04/2020 23:09
	116	30	03/05/2020 01:11
	377	3	03/07/2020 21:11

大概十几个，都是用来诈骗的

目标的桌面截图长这个吊样，下面登录着4个QQ。



诈骗分子的电脑上是没有你的通讯录备份的，一般只有你的打XX视频和果体视频



这是从诈骗分子桌面上下载回来的话术截图

A screenshot of a text file named '最新话术.txt' (Latest Script.txt). The file content is mostly illegible but appears to be a list of instructions or a script. The file icon is a document with a folded corner. Below the file icon, the text '最新话术.txt' is displayed in large white characters, followed by a small speech bubble icon and the text 'HACK学习呀'.

要不要 解决 你 跟小妹 搞 聊 打 飞机的 视频，我就图个 小财3000 钱给我了 我当你的面开视频帮你删掉你和小妹打飞机的视频 你要是不处理我立马把这个视频群发你通讯录和网上，这视频里的你拍的也很清晰，相信你朋友家人都认得出是你吧 要不要解决一句话就好！！

2、哥们视频给你删了你是不是看到了，然后还有件事跟你说下，你这个手机通讯录以及你手机信息 个人隐私删不删？删这个档案1500。

你先听我说，因为在你跟我家小妹视频的时候后台那边自动绑定了一份档案，如果后台没有收到这个钱就会在规定时间内给你通讯录一个一个发送视频直到收到这个钱为止，找你家人解决就不是1500了，是五千或者一万了。我说话也是算话的你钱到了，我还是让你看着删。

你自己好好想想，如果这个视频群发了你的通讯录，你以后怎么出去做人，你爸妈和亲人出去怎么做。为了这点小钱让 别人骂你丢人吧 1500百块钱帮你把事情处理干净了，以后也没有任何人再来打扰你了。

都是有剧本的，色字头上一把刀啊，大家一定要注意防范，后面的就不发了，全部都是话术，而且还会继续问你要钱

15、兄弟我这边跟你浪费了这么长时间，服务器暂停这，我这边员工都是干不了活了，所以说这个东西要差点一下的，兄弟我看你也是诚心解决问题，这个钱转过来就什么事都没有了最后1000

换个人接着骗你钱

跟他说我吧我电话给我老板，我老板有话跟你说，一定要说你好好跟我老板说话，我老板脾气不好。（造成个错觉，然后认为这个老板可以做出任何事来）

我是这里的老板，然后软件也是我开发的，我现在这里还有你所有资料的备份（最后一份）3000转过来，我把这个事情给你处理干净了，一会就不会再有人打扰你了。（换人说）

你以为你第一次把钱给了，对方就会放过你吗，他们还会骗你第一次第二次，直到骗干你的钱。

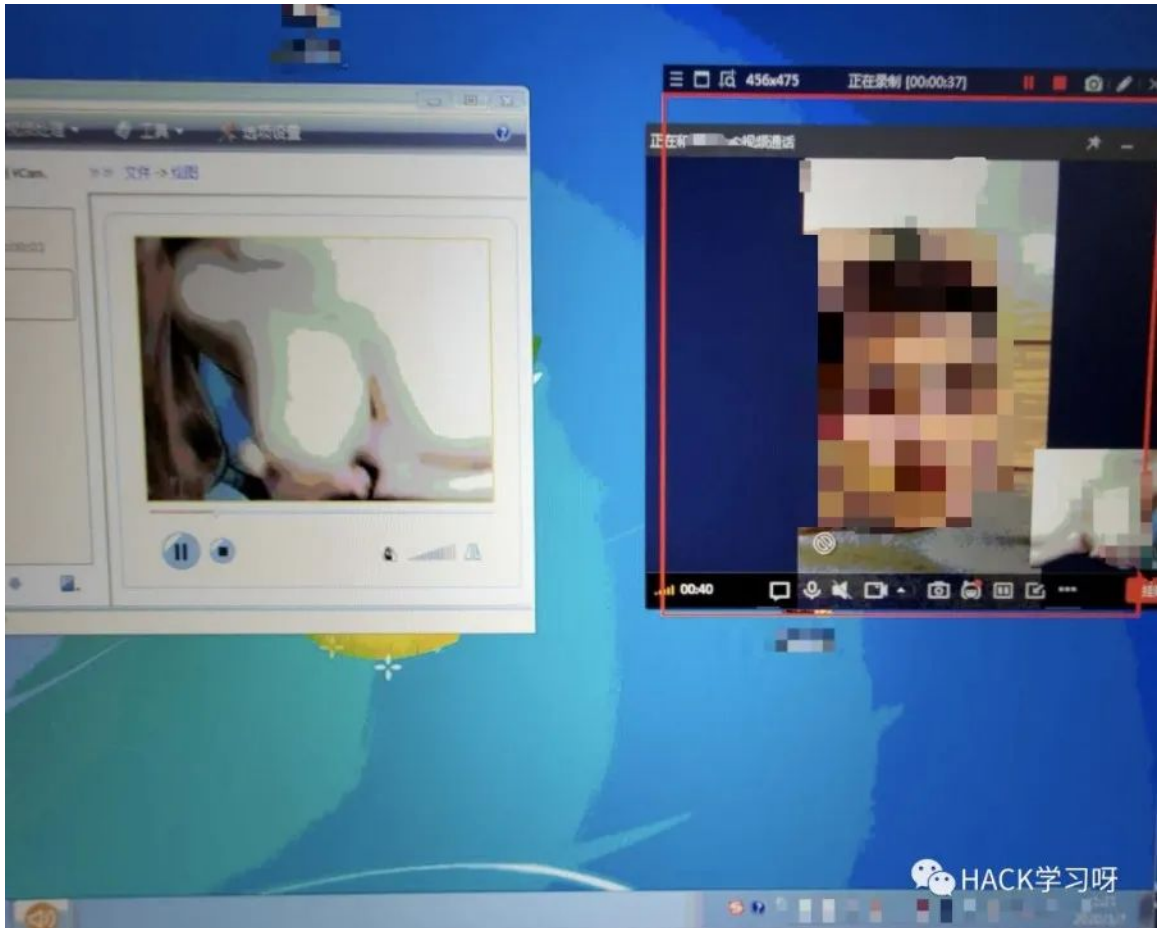
所有的套路模板都是一样的，连这个女的都一直用同一个人。



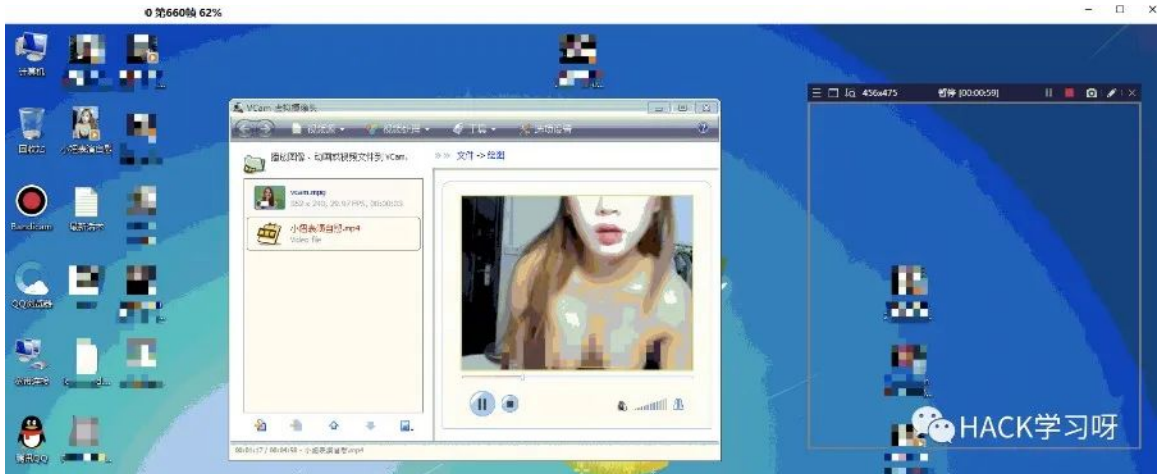
连视频都是一个人，这下你们懂了吧，管住自己的二弟，就能避免钱财损失

诈骗分子是如何用视频来和你聊天呢，通过一个软件：Vcam，把视频变成他的摄像头，然后把视频拖了进去。

对了，我们还上一个了一个远控监控了会目标的桌面，结果就直接看到了这个画面



利用虚拟的摄像头与被害人视频聊天



最后，还是那句老话

天上不会掉馅饼，努力奋斗才能梦想成真

色字头上一把刀，不是谋财就是害命
希望大家引以为戒，不要在被骗了



推荐阅读：

粉丝被裸聊勒索诈骗，我们花了2个小时黑进了骗子后台

记得三连！

精选留言

用户设置不下载评论