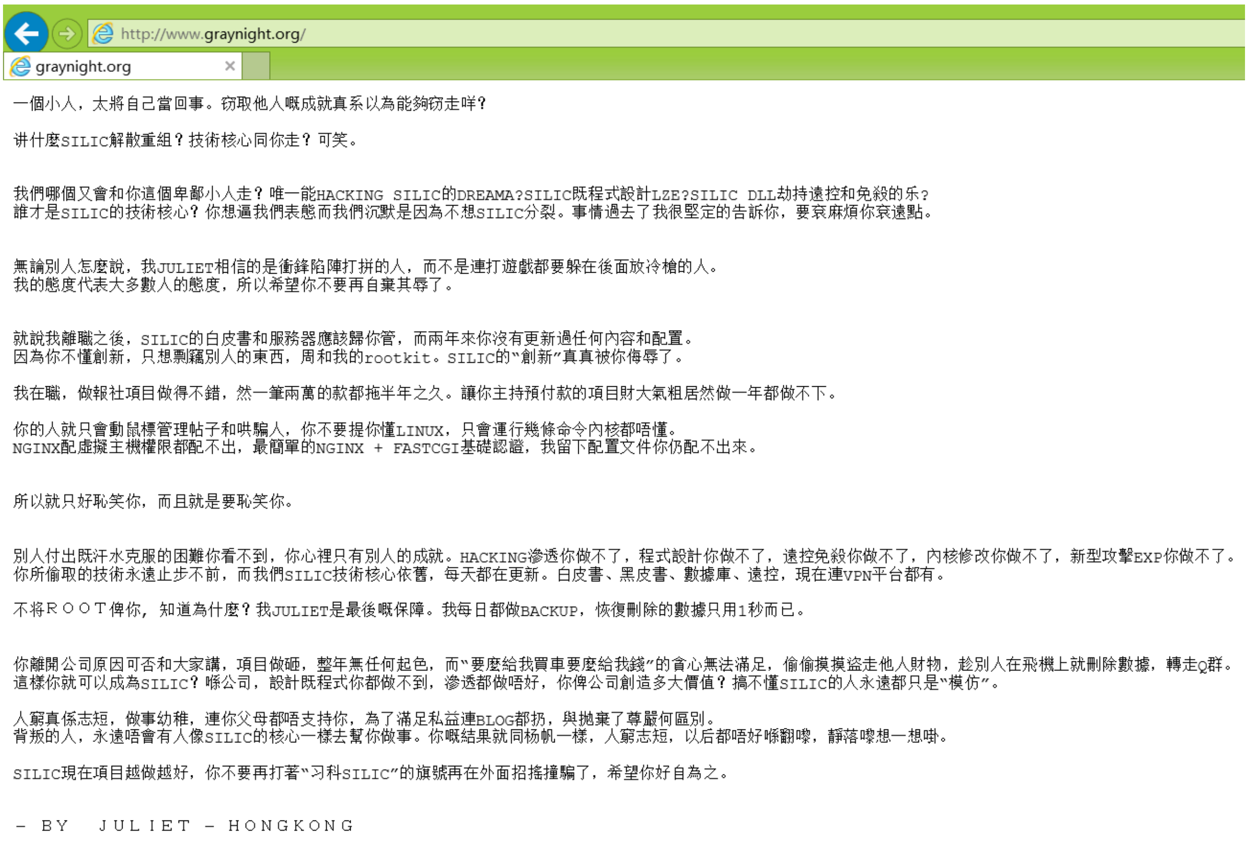
习科前员工曲振德对习科服务器攻击行为的简要取证

2015 年 2 月 13 日至 2 月 14 日，习科附件服务器遭到一定规模的 CC 攻击和 DDoS 攻击。就在 D 阔窃喜每天近 200GB 的数据量并准备挂到春节的时候，习科的技术人员已经完成闪电取证，其矛头直指习科前员工曲振德。



一個小人，太將自己當回事。竊取他人嘅成就真系以為能夠竊走咩?

讲什麼SILIC解散重組？技術核心同你走？可笑。

我們哪個又會和你這個卑鄙小人走？唯一能HACKING SILIC的DREAMA?SILIC既程式設計LZE?SILIC DLL劫持遠控和免殺的乐?
誰才是SILIC的技術核心? 你想逼我們表態而我們沉默是因為不想SILIC分裂。事情過去了我很堅定的告訴你，要衰麻煩你衰遠點。

無論別人怎麼說，我JULIET相信的是衝鋒陷陣打拼的人，而不是連打遊戲都要躲在後面放冷槍的人。
我的態度代表大多數人的態度，所以希望你不要再自棄其辱了。

就說我離職之後，SILIC的白皮書和服務器應該歸你管，而兩年來你沒有更新過任何內容和配置。
因為你不懂創新，只想剽竊別人的東西，周和我的rootkit。SILIC的〝創新〞真真被你侮辱了。

我在職，做報社項目做得不錯，然一筆兩萬的款都拖半年之久。讓你主持預付款的項目財大氣粗居然做一年都做不下。

你的人就只會動鼠標管理帖子和哄騙人，你不要提你懂LINUX，只會運行幾條命令內核都唔懂。
NGINX配虛擬主機權限都配不出，最簡單的NGINX + FASTCGI基礎認證，我留下配置文件你仍配不出來。

所以就只好恥笑你，而且就是要恥笑你。

別人付出既汗水克服的困難你看不到，你心裡只有別人的成就。HACKING滲透你做不了，程式設計你做不了，遠控免殺你做不了，內核修改你做不了，新型攻擊EXP你做不了。
你所偷取的技術永遠止步不前，而我們SILIC技術核心依舊，每天都在更新。白皮書、黑皮書、數據庫、遠控，現在連VPN平台都有。

不將ＲＯＯＴ俾你，知道為什麼？我JULIET是最後嘅保障。我每日都做BACKUP，恢復刪除的數據只用1秒而已。

你離開公司原因可否和大家講，項目做砸，整年無任何起色，而〝要麼給我買車要麼給我錢〞的貪心無法滿足，偷偷摸摸盜走他人財物，趁別人在飛機上就刪除數據，轉走Q群。
這樣你就可以成為SILIC？喺公司，設計既程式你都做不到，滲透都做唔好，你俾公司創造多大價值？搞不懂SILIC的人永遠都只是〝模仿〞。

人窮真係志短，做事幼稚，連你父母都唔支持你，為了滿足私益連BLOG都扔，與拋棄了尊嚴何區別。
背叛的人，永遠唔會有人像SILIC的核心一樣去幫你做事。你嘅結果就同杨帆一樣，人窮志短，以后都唔好嚟翻嚟，靜落嚟想一想啦。

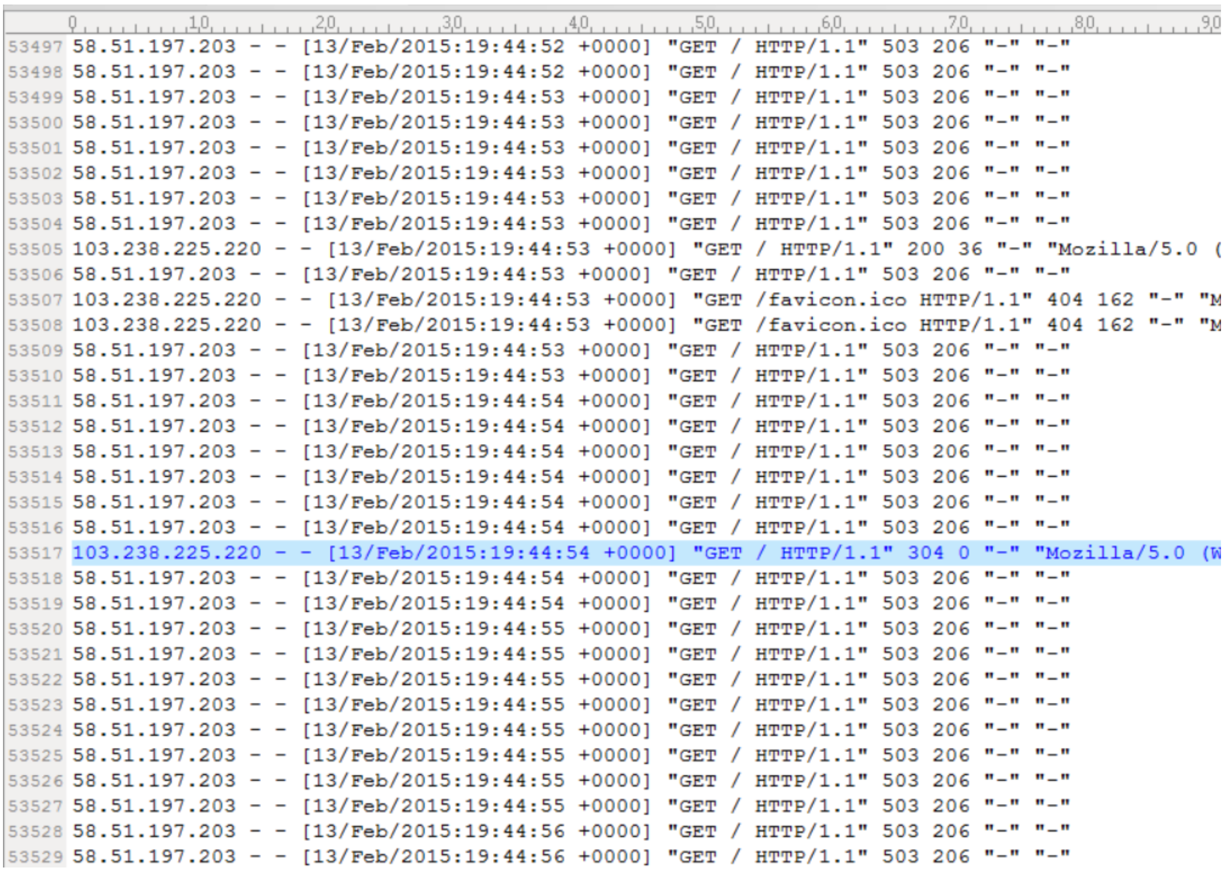
SILIC現在項目越做越好，你不要再打著〝习科SILIC〞的旗號再在外面招搖撞騙了，希望你好自為之。

－ BY JULIET － HONGKONG

在此，习科想说，偷走公司桌椅台式机进行时所谓的“创业”，糊弄不明真相的人，已经很丢人了，不要再一而再再而三的做丢人的事了。

具体细节见下文。

从 2 月 13 日夜里开始，习科服务器 WAF 预警就开始提示，直到 14 日中午，服务器单日流量达到平均 200GB。日志节选如下：



```
58.51.197.203 - - [13/Feb/2015:19:44:52 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:52 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
103.238.225.220 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 200 36 "-" "Mozilla/5.0 (
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
103.238.225.220 - - [13/Feb/2015:19:44:53 +0000] "GET /favicon.ico HTTP/1.1" 404 162 "-" "M
103.238.225.220 - - [13/Feb/2015:19:44:53 +0000] "GET /favicon.ico HTTP/1.1" 404 162 "-" "M
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
103.238.225.220 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (W
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:55 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:56 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
58.51.197.203 - - [13/Feb/2015:19:44:56 +0000] "GET / HTTP/1.1" 503 206 "-" "-"
```

从日志可以看到一个 ip：103.238.225.220 的访问者。从 CC 攻击开始前，其访问了习科服务器一次。

在 CC 攻击开始后，该 ip 曾多次试探访问习科服务器。

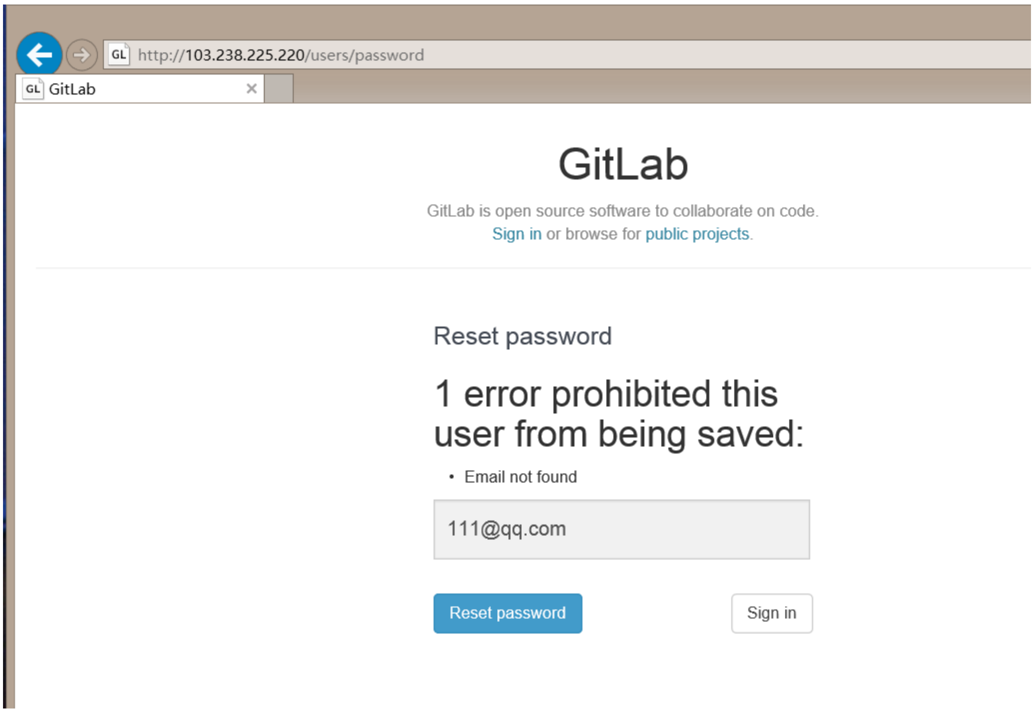
访问日志对 103.238.225.220 进行了筛选(HTTP 304 状态可视为 200 状态)

```
103.238.225.220 - - [13/Feb/2015:19:43:19 +0000] "GET / HTTP/1.1" 200 1789 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:43:19 +0000] "GET /favicon.ico HTTP/1.1" 404 162 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:43:20 +0000] "GET /favicon.ico HTTP/1.1" 404 162 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:43:31 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
```

```
103.238.225.220 - - [13/Feb/2015:19:44:03 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:44:19 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:44:19 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:44:53 +0000] "GET / HTTP/1.1" 200 36 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"103.238.225.220 - - [13/Feb/2015:19:44:53 +0000] "GET /favicon.ico HTTP/1.1" 404 162 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:44:53 +0000] "GET /favicon.ico HTTP/1.1" 404 162 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
103.238.225.220 - - [13/Feb/2015:19:44:54 +0000] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:35.0) Gecko/20100101 Firefox/35.0"
```

通过调研，我们认为只要确认了该 VPS 的所属者就确认了攻击源。

该服务器开放了 80 端口，装了类似 SVN 的源码平台。要确认该服务器的归属其实很简单。



GitLab

GitLab is open source software to collaborate on code.
Sign in or browse for public projects.

Reset password

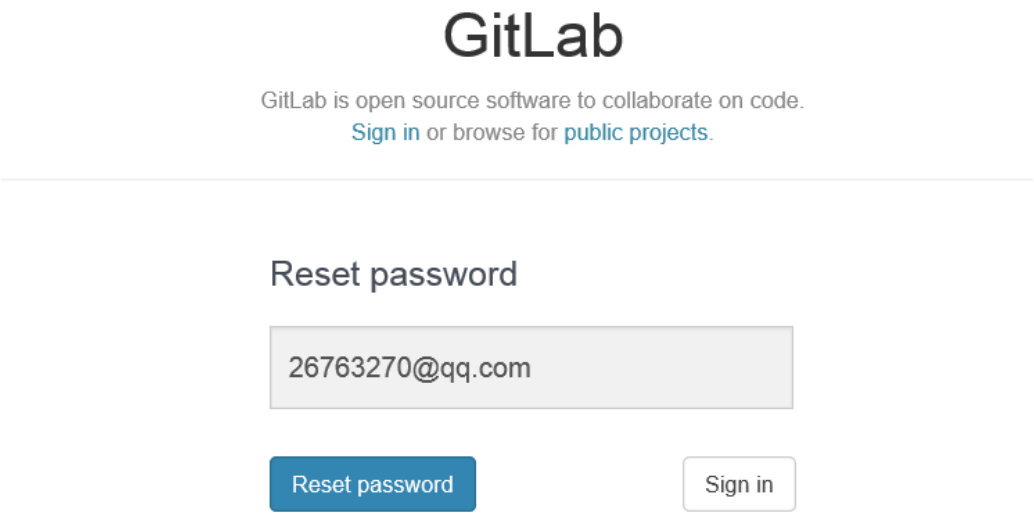
1 error prohibited this user from being saved:

- Email not found

111@qq.com

该平台存在一个“Reset Password”，当输入的邮箱是随机一个邮箱时，返回的“ERROR”信息。

但是如果输入一个人的邮箱像这样：



GitLab

GitLab is open source software to collaborate on code.
Sign in or browse for public projects.

Reset password

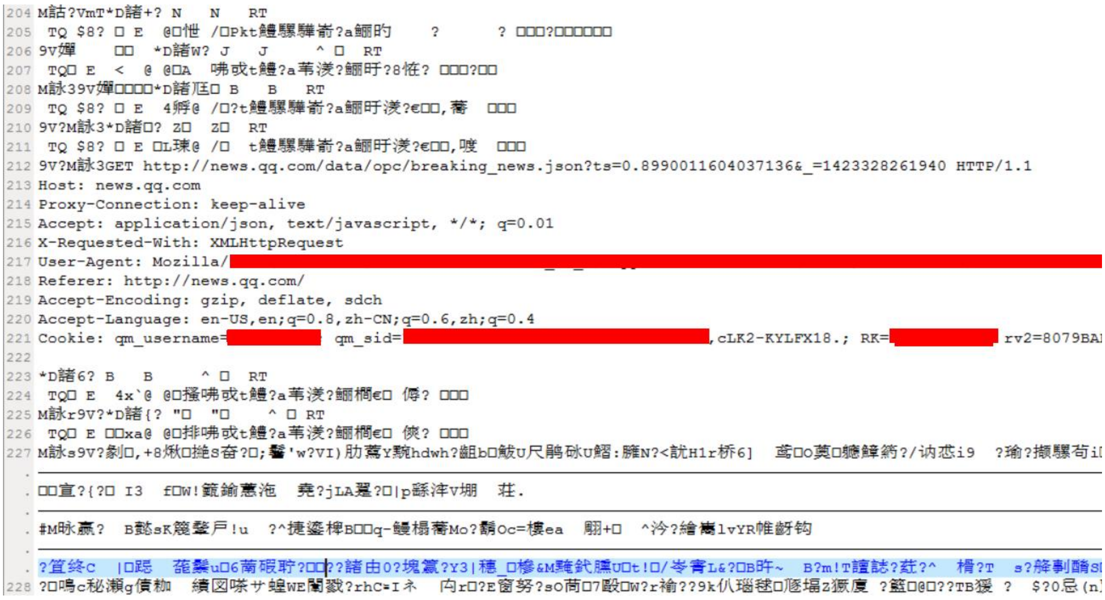
26763270@qq.com

系统返回登陆界面，默认为找回密码的邮件已经发送。

当然了，这些并不足以成为铁证。曲振德利用的大部分肉鸡都是 edu.cn 的机器，再后面的取证可以参加针对黑客“M3QD4D”的取证，简单的入侵手法获得肉鸡(肉鸡列表将会发到习科论坛，有兴趣的可以测试)。

除此以外，在黑板报前一篇所讲的 CICC 机器上“/usr/bin”目录下发现代理后门，程序名为 cow。

该后门在 Git 上面我们找到了源码，并做了修改，记录下一些访问内容如图。



```
M詁?VmT*D諸+? N    N    RT
 TQ $8? □ E  @□怈 /□Pkt饇驟驊嵛?a鰤旳     ?       ? □□□?□□□□□□
9V嬋      □□  *D諸W? J    J      ^ □  RT
 TQ□ E  <  @ @□A  咈或t饇?a苇淩?鰤旴?8恠? □□□?□□
M詠39V嬋□□□□*D諸尫□ B    B    RT
 TQ $8? □ E  4孵@ /□?t饇驟驊嵛?a鰤旴淩?€□□,蕎   □□□
9V?M詠3*D諸□? Z□  Z□  RT
 TQ $8? □ E □L琜@ /□  t饇驟驊嵛?a鰤旴淩?€□□,嗖   □□□
9V?M詠3GET http://news.qq.com/data/opc/breaking_news.json?ts=0.8990011604037136&_=1423328261940 HTTP/1.1
Host: news.qq.com
Proxy-Connection: keep-alive
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/[redacted]
Referer: http://news.qq.com/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8,zh-CN;q=0.6,zh;q=0.4
Cookie: qm_username=[redacted]  qm_sid=[redacted],cLK2-KYLFX18.; RK=[redacted] rv2=8079BA

*D諸6? B    B      ^ □  RT
 TQ□ E  4x`@ @□搔咈或t饇?a苇淩?鰤椆€□ 僔? □□□
M詠r9V?*D諸{? "□   "□     ^ □ RT
 TQ□ E □□xa@ @□排咈或t饇?a苇淩?鰤椆€□ 倈? □□□
M詠s9V?劀□,+8烑□撟S奋?□;鬠'w?VI)肋蔫Y敤hdwh?齟b□鮁U尺鹃砯U鰫:臃N?<訧H1r桥6]   鸢□O莫□戅饆絎?/讷恋i9  ?瑜?擷驟苟i
□□亶?{?□ I3  f□W!簏鍮蕙洈   堯?jLA翯?□|p蘨洋V堋  荘.
#M昹赢?  B懿sK籛鍪戸!u  ?^捷鎏榫B□□q-鳗楊蕎Mo?翾Oc=樓ea   翢+□  ^泠?繪蔥1vYR帷齖钩
?笪终C  |□跽   蓶鬃u□6萳碬聍?□□??諸由0?塊篢?Y3|穗_□椮&M黐鈫膔U□t!□/岺審L&?□B昨~  B?m!T譠誌?葤?^  楫?T  s?觪剬醐S
?□嗚c秘瀨g僨枷   續図嗏サ蝗WE闈戮?rhC=Iネ   内r□?E窗努?sO苘□7毆□W?r褕??9k仈瑙毯□陓塥Z搋厪 ?籃□@□??TB猨 ?  $?0忌(n
```

具体 Linux 服务器后门相关技术内容，将择日在习科论坛发布。每一篇所涉及的技术内容可能不多，但是习科更注重讲思路，多篇组合起来希望对大家有所帮助。

本文阐述主要取证思路

DDoS 和 CC 攻击一直都是令无数管理员头疼的事，习科遇到这种事其实也很头疼，但是追查其攻击源是习科公司的业务范围之一。D 阔在对某些目标进行攻击前，一定会对其踩点，耐心和细心的日志筛选，是获得攻击者重要信息的手段之一。例如黑客上次对习科进行 CC 攻击的工具使用的是 mtsb.cn 的工具，黑客圈就这么大，谁用什么东西攻击什么地方，其实不用细查也知道是谁。

在其使用的代理服务器上对程序进行修改、监听，也是取证手段之一，D 阔为了满足数量的需要，其肉鸡的安全程度必然比普通入侵得来的肉鸡更脆弱。

小编写在最后

习科前网站管理员曲振德在习科主管在回国飞机上劫持习科域名及 QQ 群，跳转至自己新建的所谓的“习科”站点上，趁公司主管不在，偷走公司桌椅、台式机甚至烧掉的 XBox，本已经够丢人了。

之所以对刑事犯罪行为不追究，一来是念及创业情分，二来给一些人留一些脸面，如果不讲情面，PDF 详细报告就已经公开下载了。

习科公司 2014 年曲振德主持的开发项目亏损几十万，带领的技术团队在安全上没有任何技术革新，还要求年底要么配车要么折现金，因为公司做不到于是就有了“习科联创”。

QQ 截图当然都是截对自己有利的地方，习科公司也可以调出公司沙龙时候曲振德父母来青岛入住四星酒店及餐厅的登记账单，以及各种证明“习科没有对不起曲振德”的证据，之所以没有这么做，好话都让你去说，无非是觉得无论什么事，无论双方哪方，做事还该给自己留点脸。

习科从一个民间兴趣团体成长为一个有技术积累的安全厂商，并不仅仅是靠几个技术核心的倚老卖老，走了很多人也来了很多人，如果非要把走到人归咎到主管的不好，把来的人算做某一个人的功劳，那么习科走不长远。

其他的话习科前技术主管 Juliet 早已经放在曲振德曾经的个人博客 graynight.org 上面了，你应该很清楚你耍赖也好阴人也好，习科不是拿你没辙，希望你好自为之。

技术的车轮滚滚向前，习科不会因为盗窃，剽窃，攻击，诽谤而止步不前，习科的技术核心会把精力投入到技术研究和革新上。

我们会一如既往的向大家分享技术经验、研究结果。