Who is Mr Zeng?

intrusiontruth.wordpress.com/2019/07/22/who-is-mr-zeng/

intrusiontruth July 22, 2019

In previous articles we identified Jinan Quanxin Fangyuan Technology Co. Ltd. (济南全欣方沅科技有限公司), Jinan Anchuang Information Technology Co. Ltd. (济南安创信息科技有限公司) and Jinan Fanglang Information Technology Co. Ltd. (济南方朗信息科技有限公司) as companies associated with Guo Lin (郭林), a likely MSS Officer in Jinan. We also identified an IT Security expert from Jinan, Wang Qingwei (王庆卫), as the representative of the Jinan Fanglang company. Another, potentially separate, individual goes by the name 'iamjx'.

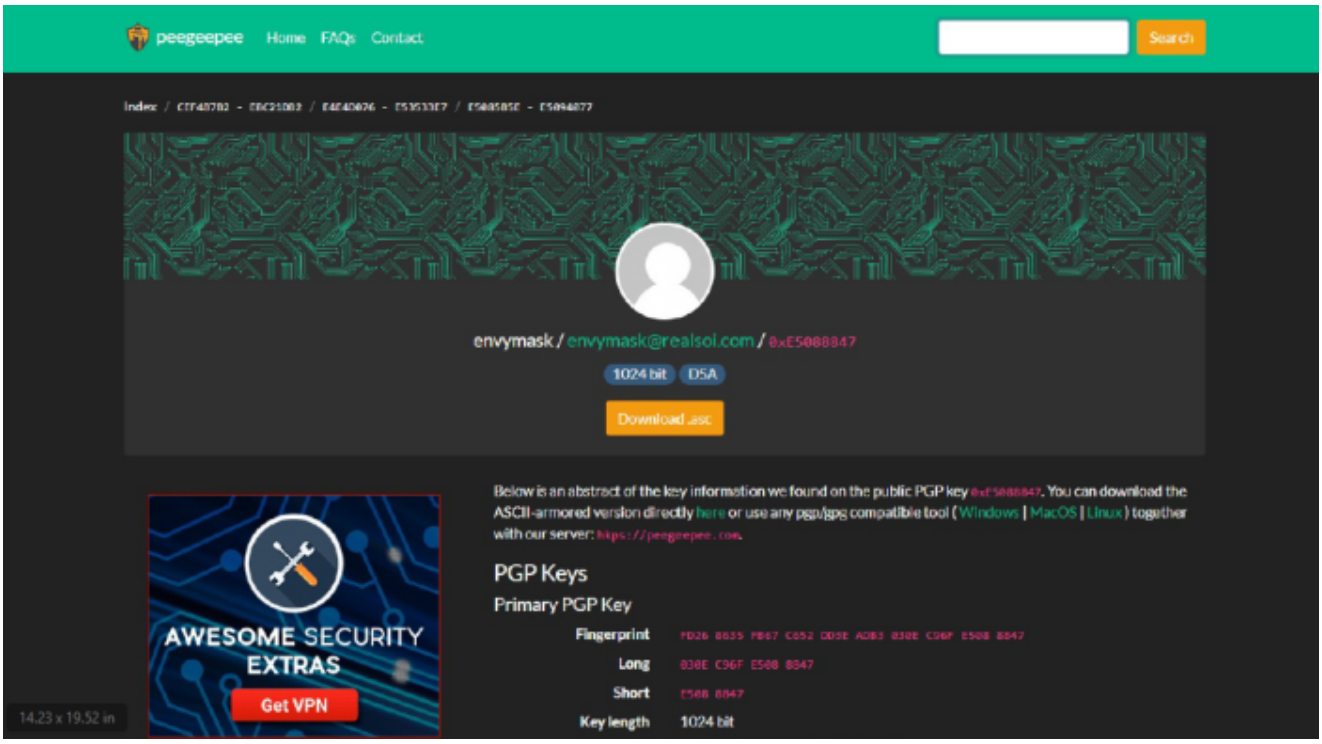
The identification of further individual in Jinan requires us to follow the trail from what we believe to be a *fourth* front company.

RealSOI Computer Network Technology Company

A different analyst providing information to this blog identified RealSOI Computer Network Technology Company (瑞索计算机网络科技有限公司) as a company closely related to Jinan Quanxin, Jinan Anchuang and Jinan Fanglang. Our team spent some time researching links between the companies and identifying staff linked to RealSOI who were associated with hacking activity.

Information in open source on RealSOI is limited, but Chinese recruitment websites indicate that RealSOI operates from 66, Shanda South Road, Lixia District, Jinan. Our analysts also identified a website (realsoi[.]com) archived on archive.org, showing the company claiming to offer research in areas such as Computer Criminal Forensics, High-Performance Computing and Social Operating Systems.

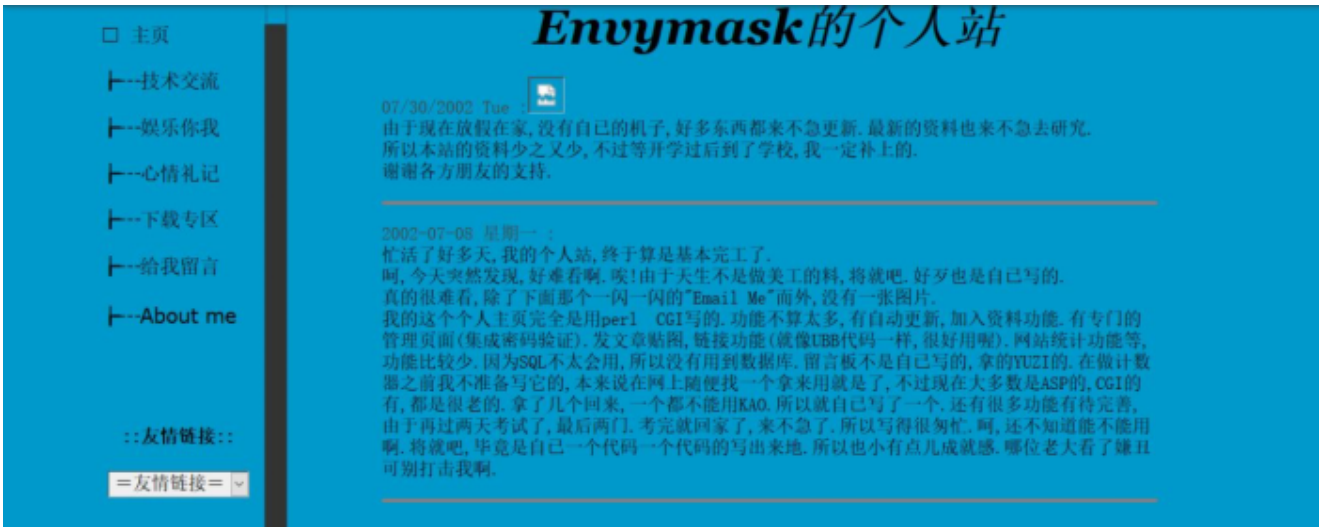
Archived copy of realsoi[.]com**envymask**
Our open source investigation identified a single PGP key associated with the realsoi[.]com domain in the name ‘envymask’.



PGP key associated with envymask and RealSOI
envymask is a well-known member of Chinese hacking circles and is a member of the ph4nt0m group. In this post, using e-mail account 13[at]21cn.com, he promotes the 20cn[.]org security group for discussion of hacking topics in China. He appears to have a senior role within the group as joint author of the post with ‘PsKey’.

envymask and PsKey on CSDN

envymask had his own website back in 2002, a copy of which was captured by archive.org. He doesn't give his name on the site, but he does give some of his biographical background, including a date of birth in 1980 in Sichuan province and details of studies at the Nanjing Science and Engineering University in 1999. Nanjing, of course, is where likely MSS Officer Guo Lin studied, and from where he published his IT Security paper, detailed in an earlier article.



envymask's biography on his personal website

Zeng Xiaoyong (曾小勇)

As you've no doubt guessed, envymask has a real name. He is Zeng Xiaoyong (曾小勇). According to information provided to us by a source with access to information in China, Zeng Xiaoyong was born on 22 November 1980 and worked at RealSOI in the mid-2000s.

MS08-067

envymask isn't just any mediocre Chinese hacker. In this online post, in which he also uses the name 'EMM', he claims to be the author of the MS08-067 exploit for Chinese operating systems. Presumably this means he ported it to the Chinese version of Windows. The generic version of MS08-067 is a well-known exploit used in multiple attacks including the Conficker worm.

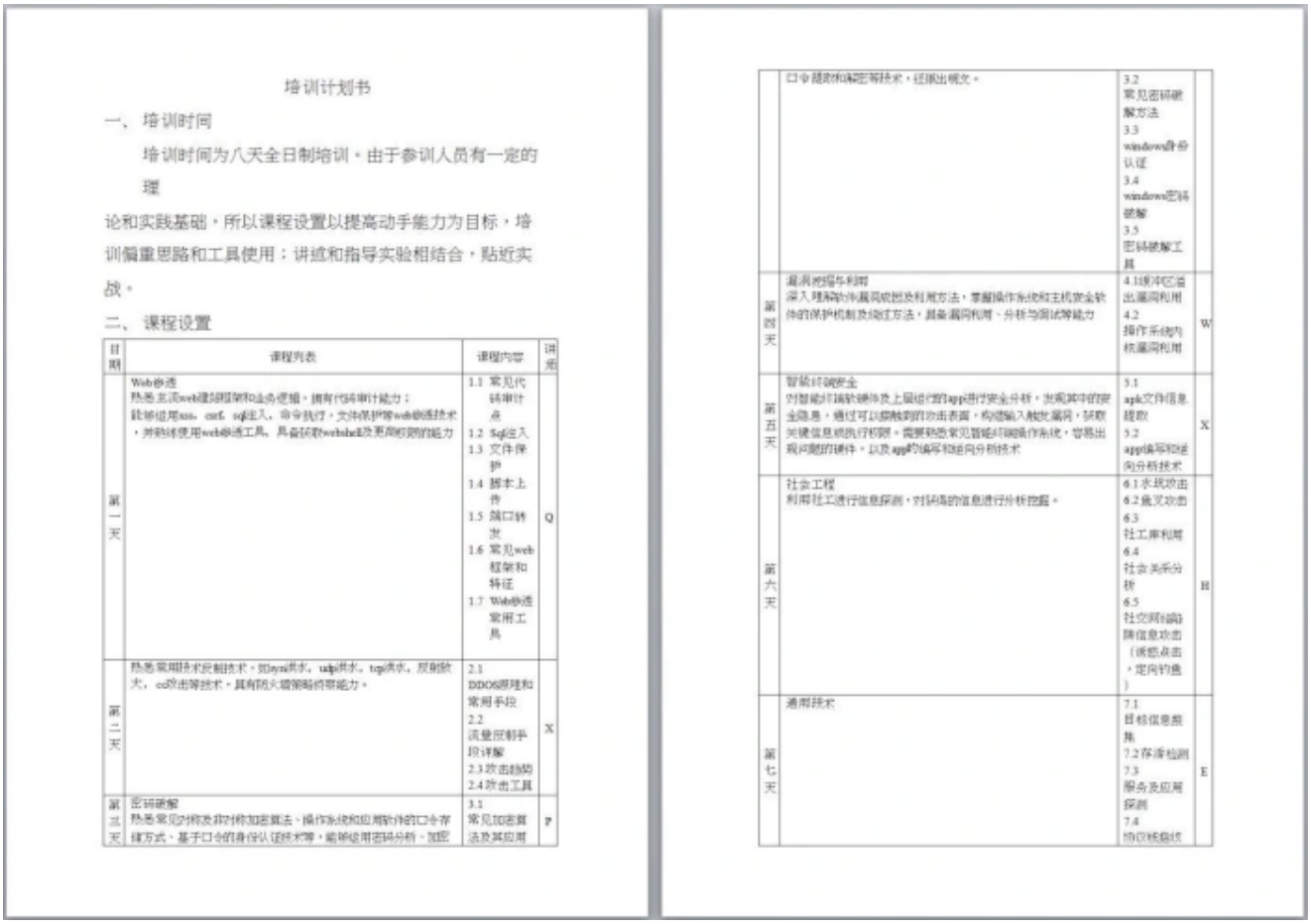
No.40.emm

写了这么多差点把自己写掉了，请允许我把自己的名字写这儿，我真的、真的愿意做大家成功道路上的一颗垫脚石，一颗永远不需要闪光的垫脚石，我愿意看着你们一个一个的走向成功的道路，同时也希望不久的将来能把你的名字写上去，去为龙的传人争光，我叫envymask，小黑客们用的那个ms08067 exp就是我写的。

envymask, EMM, as author of MS08-067

So, does Zeng Xiaoyong know Wang Qingwei?

The answer to that is yes. The images below are from a training plan associated with Jinan Fanglang. Those with a keen eye will spot that 'EMM', listed as responsible for the MS08-067 exploit, is one of the trainers. Who else is listed on the course as a trainer? 'Phoenix', which you will remember was a name used by Wang Qingwei when recruiting for Jinan Fanglang.



培训计划书

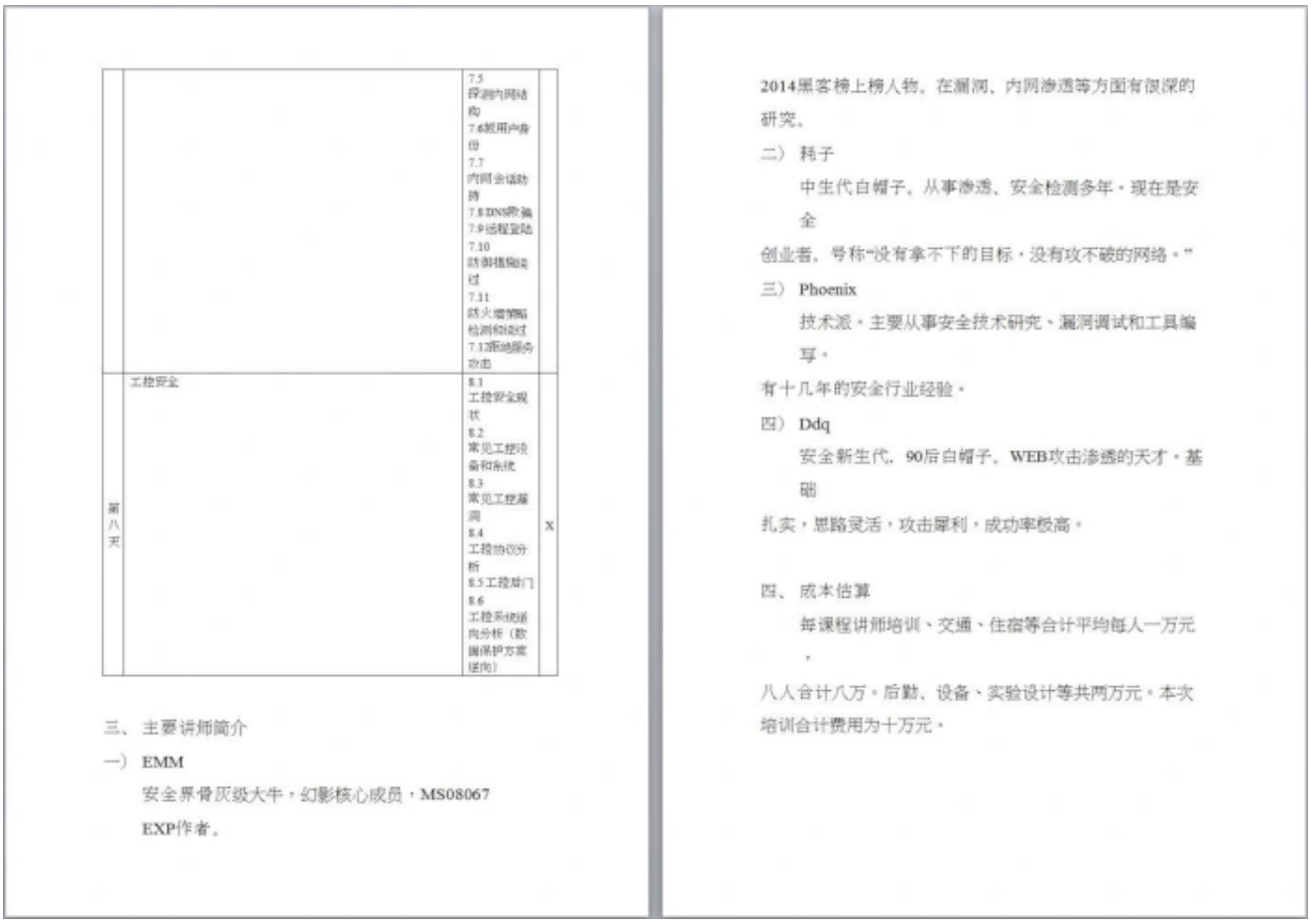
一、培训时间

培训时间为八天全日制培训。由于参训人员有一定的理

论和实践基础，所以课程设置以提高动手能力为目标，培训偏重思路和工具使用；讲述和指导实验相结合，贴近实战。

二、课程设置

日期	课程列表	课程内容	讲师
第一天	Web渗透 熟悉主流web建站框架和业务逻辑，拥有代码审计能力； 能够运用xss、csrf、sql注入，命令执行，文件保护等web渗透技术，并熟练使用web渗透工具，具备获取webshell及更高权限的能力	1.1 常见代码审计点 1.2 Sql注入 1.3 文件保护 1.4 脚本上传 1.5 端口转发 1.6 常见web框架和特征 1.7 Web渗透常用工具	Q
第二天	熟悉常用防反制技术，如iptables防火，tcp防火，反制防火，cc攻击等技术，具有防火墙策略编写能力。	2.1 DDOS原理和常用手段 2.2 流量反制手段详解 2.3 攻击脚本 2.4 攻击工具	X
第三天	密码破解 熟悉常见的哈希加密算法，操作系统和应用软件的口令存储方式，基于口令的身份认证技术等，能够运用密码分析、加密	3.1 常见加密算法及其应用	P
	口令猜测和解密等技术，还很出彩。	3.2 常见密码破解方法 3.3 windows身份认证 3.4 windows密码破解 3.5 密码破解工具	
第四天	漏洞的编写利用 深入理解软件漏洞原理及利用方法，掌握操作系统和主机安全软件的保护机制及绕过方法，具备漏洞利用、分析与测试等能力	4.1缓冲区溢出漏洞利用 4.2 操作系统内核漏洞利用	W
第五天	智能终端安全 对智能终端软硬件及上层运行的app进行安全分析，发现其中的安全隐患，通过可以触发的攻击表面，构造输入触发漏洞，获取关键信息或执行权限。需要熟悉常见智能终端操作系统，容易出现问题的硬件，以及app的编写和逆向分析技术	5.1 apk文件信息提取 5.2 app编写和逆向分析技术	X
第六天	社会工程 利用社工进行信息探测，对码高的信息进行分析挖掘。	6.1 水坑攻击 6.2 鱼叉攻击 6.3 社工库利用 6.4 社会关系分析 6.5 社交网络陷阱信息攻击（诱惑点击，定向钓鱼）	H
第七天	通用技术	7.1 目标信息搜集 7.2 存活检测 7.3 服务及应用探测 7.4 协议栈指纹	E



		7.5 探测内网结构 7.6 抓用户身份 7.7 内网金钱劫持 7.8 DNS欺骗 7.9 远程登陆 7.10 防御措施绕过 7.11 防火墙策略检测和绕过 7.12 拒绝服务攻击	
第八天	工控安全	8.1 工控安全现状 8.2 常见工控设备和系统 8.3 常见工控漏洞 8.4 工控协议分析 8.5 工控防火墙 8.6 工控系统渗透分析（数据保护方案渗透）	X

三、 主要讲师简介

一） EMM

安全界骨灰级大牛，幻影核心成员，MS08067 EXP作者。

2014黑客榜上榜人物。在漏洞、内网渗透等方面有很深的研究。

二） 耗子

中生代白帽子。从事渗透、安全检测多年。现在是安全创业者。号称"没有拿不下的目标，没有攻不破的网络。"

三） Phoenix

技术派。主要从事安全技术研究、漏洞调试和工具编写。有十几年的安全行业经验。

四） Ddq

安全新生代，90后白帽子。WEB攻击渗透的天才。基础扎实，思路灵活，攻击犀利，成功率极高。

四、 成本估算

每课程讲师培训、交通、住宿等合计平均每人一万元，八人合计八万。后勤、设备、实验设计等共两万元。本次培训合计费用为十万元。

Jinan Fanglang training plan showing ‘EMM’ and ‘phoenix’ as trainers

The Phreaker (耗子)

The second trainer listed at the end of the training document, between EMM and Pheonix, is **耗子** (Haozi). **耗子** translates literally into English as ‘rat’ or ‘mouse’, but you will recognise the format of the name from the ‘reservoir dogs’ QQ names used in the Antorsoft group. **耗** is Chinese for ‘consumption’ and **耗子** is used as a shortened version of ‘电话耗子’ (telephone mouse). The English translation is ‘phreaker’, a form of hacker in the 1980s that found ways to use dial up connections for free, effectively stealing telephone company resources.

有许多不同的术语用于描述那些闯入电话网络或数据网络的人。那些操作电话连接或资源供自己利用的人被称为“电话耗子”（phone phreak）或“耗子”（phreaker）。“黑客”（hacker）的最初含义是掌握计算机硬件和软件的内部工作以便更好地领会的人。被称为黑客在过去是一种恭维，反映了一个人非凡的计算机技能。为了将黑客与使用计算机技能实施恶意行为的人区别开来，我们把那些设法破坏数据或系统的人称为“解密高手”（cracker）。不过，现在有许多人同时使用 hacker 和 cracker。许多远程通信专家已经将 hacker 这个词确定为“电话耗子”的术语——各种各样的黑客。为了简单起见，本章也使用这个术语来描述获得了对语音和数据网络的未授权访问的人，无论它是否怀有恶意。

Explanation of ‘phreaker’ in Chinese telecommunications textbook

In summary, Zeng Xiaoyong, a well-known Chinese hacker using the handles ‘envymask’ and ‘EMM’ worked for RealSOI. RealSOI was closely associated with the MSS front companies identified in previous articles and Zeng knew Wang Qingwei, having worked as an InfoSec trainer with him.

#youknowwherethisleads