Who is Mr Guo?

intrusiontruth.wordpress.com/2019/07/17/who-is-mr-guo/

intrusiontruth July 17, 2019

In our last post, we stated that a source whose identity we had verified had named an MSS Officer in Jinan who was believed to be involved in Cyber operations. We are now in a position to reveal that the name provided to us is 郭林 (Guo Lin). Open source research conducted by analysts working for Intrusion Truth quickly revealed a potential candidate for Guo Lin.

Guo Lin, Masters Student

An IT security paper from 2007 called '基于多维角度的攻击分类方法' (Method of Classifying Attacks Based on Multi-dimension) was authored by a Guo Lin in which he described himself as a Masters student conducting research into network and information security and malicious code detection. Guo was a Computer Science student at Nanjing University (not Jinan), making it uncertain whether he is indeed the same individual in Jinan named in our tip.

There is nothing wrong with being a Masters student, of course. So let's take a look at what else Guo has been up to.

glince[at]163.com

Our high confidence that we have the right person comes from the e-mail address used by Guo in the paper – glince[at]163.com. We will show how the e-mail address links Guo to Jinan.

第 24 卷第 4 期
2007 年 4 月

计 算 机 应 用 研 究
Application Research of Computers

Vol. 24, No. 4
April 2007

基于多维角度的攻击分类方法*

郭 林[1,2], 严 芬[1,2,3], 黄 皓[1,2]

(1. 南京大学 软件新技术国家重点实验室, 江苏 南京 210093; 2. 南京大学 计算机科学与技术系, 江苏 南京 210093; 3. 扬州大学 信息工程学院 计算机科学与工程系, 江苏 扬州 225009)

摘 要: 提出了一种新的基于多维角度的攻击分类方法,给出分类的标准和结果。通过对诸多攻击样例的分类来验证所给的攻击分类方法,并对此攻击分类的方法作了客观的分析评价。

关键词: 安全; 攻击; 攻击分类; 分类原则; 分类标准

中图分类号: TP393.08 文献标志码: A 文章编号: 1001-3695(2007)04-0139-05

Method of Classifying Attacks Based on Multi-dimension

GUO Lin[1,2], YAN Fen[1,2,3], HUANG Hao[1,2]

(1. *State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing Jiangsu 210093, China*; 2. *Dept. of Computer Science & Technology, Nanjing University, Nanjing Jiangsu 210093, China*; 3. *Dept. of Computer Science & Engineering, Institute of Information Technology, Yangzhou University, Yangzhou Jiangsu 225009, China*)

Abstract A new attack classification method was put forward and delivered the criterion and results of the classification. This method is validated by classifying many attack samples. At the same time, an objective analysis and estimate of this classification method were given.

Key words: security; attacks; attack classification; classification principle; classification criterion

0 引言

在计算机技术和网络技术发展及应用范围不断扩大的同时,对计算机和网络的攻击也日益增长。根据美国权威安全事件应急处理组织 CERT/CC 最新发布的统计报告[1],2003 年 CERT/CC 受理的安全事件报告达到了 137 529起,比 2002 年增加了 50% 以上。

对计算机系统产生的一次危害可能由一个攻击行为或一系列的攻击行为造成。攻击技术发展迅速,迫切需要对攻击行为进行深入细致的研究和分析,以便及时发现攻击行为的发生,发掘攻击行为之间内在联系,从而有效地检测和对抗攻击,减小攻击造成的危害。目前,各种不同攻击检测和防御产品大量出现,但是,由于当前研究人员对攻击理解的差异,对攻击的判定和特征提取方法的不同,给各防御系统之间的交互和协作带来了困难。研究攻击分类能有效地解决上述问题。对攻击合理分类是研究攻击的前提,它可以为攻击提供统一的描述语言,便于不同研究组织之间进行交流;使用系统的方法来认识、描述攻击有利于简化对攻击的理解,把握攻击的本质特征和基本原理,更好地检测和防御攻击。

近几年来,关于计算机和网络攻击以及攻击分类方法的研究,为攻击分类的研究作出了不少贡献。但是,这些分类方法主要存在着以下几方面的缺点:①对网络攻击事件的分类随意性很强;②对同样的攻击事件判定结果不同;③对于网络攻击事件所造成的危害和潜在的危险缺乏统一的度量准则。研究攻击分类的目的是为了给出一个普遍适用的认识和理解攻击的框架。本文提出了一种新的攻击分类方法。这个分类方法主要是在对目前已存在攻击的研究的基础上提出的。分类的结果也同样适用于对未出现的攻击进行分类和系统的描述。

1 相关工作

1.1 攻击分类的基本原则

20 世纪 90 年代中后期,研究人员对攻击分类的原则进行了较多的探讨[2~4]。研究者们从不同角度考虑攻击分类。文中提出攻击分类应该遵循的原则主要有以下几条:

(1) 互斥性——各类别应是互斥的,没有交叉和覆盖现象;

(2) 穷举性——全部类别包含所有类型攻击;

(3) 无二义性——各类别精确、清晰,没有不确定性;

(4) 可重复性——不同人根据同一原则重复分类的过程,得出的分类结果应该一样;

(5) 可接受性——分类符合逻辑和事实,易于被大多数人接受;

(6) 可用性——分类对不同领域的应用具有实用价值;

(7) 适应性——可适应于多个不同应用要求;

收稿日期: 2006-02-13; 修回日期: 2006-04-14 基金项目: 国家"863"计划资助项目(2003AA142040); 江苏省高技术研究计划资助项目(BG2004030)

作者简介: 郭林(1976-),男,工程师,硕士研究生,主要研究方向为网络与信息安全,易意代码检测(glince@163.com);严芬(1978-),女,讲师,博士研究生,主要研究方向为网络与信息安全;黄皓(1957-),教授,博导,博士,主要研究方向为网络与信息安全。

Guo Lin's academic paper showing his e-mail address
antorsoft[.]com

Historical WHOIS data shows that the e-mail address glince[at]163.com was the original registrant of a number of domain names and was the admin contact for antorsoft[.]com.

```
Domain Name.................. antorsoft.com
 Creation Date.............. 2008-12-21 21:56:08
 Registration Date.......... 2008-12-21 21:56:08
 Expiry Date................ 2009-12-21 21:56:08
 Organisation Name.......... JiNan QuanXinFangYuan Tech Co.Ltd
 Organisation Address....... No 238 Jing Shi Dong Lu
 Organisation Address.......
 Organisation Address....... JiNan
 Organisation Address....... 250000
 Organisation Address....... SD
 Organisation Address....... CN

Admin Name................... Guo Lin
 Admin Address.............. No 238 Jing Shi Dong Lu
 Admin Address..............
 Admin Address.............. JiNan
 Admin Address.............. 250000
 Admin Address.............. SD
 Admin Address.............. CN
 Admin Email................ glince@163.com
 Admin Phone................ +86.53168690179
 Admin Fax.................. +86.53168690179
```

Antorsoft historical WHOIS

Jinan Quanxin Fangyuan Technology Co. Ltd.

Domain registration information for antorsoft[.]com names the registrant as Jinan Quanxin Fangyuan Technology Co. Ltd, which translates into Chinese as 济南全欣方沅科技有限公司. The address is listed as 238, Jing Shi Dong Lu, Jinan, 250000, Shandong, China. Importantly, this company is based in Jinan, just where our tip said Guo Lin was based.

Another Chinese website lists a different address for the same company at No. 12, Qilihe Road, Licheng District, Jinan, Shandong:

基本信息

企业名称：	济南金欣方元科技有限公司
名称拼写：	ji na quan xin fang yuan ke ji you xian gong si
联系人：	成松
联系电话：	***65064220
传真号码：	***65064220
城市区号：	0531
Q Q号码：	未获取
微信号码：	无
注册资本：	未填写
年营业额：	暂未获取
注册人数：	50-100人左右(人)
总和资产	无信息
电子邮箱：	***65064220@qq.com
手机号码：	*****
企业模式：	服务型企业
所在省份：	山东企业大全-济南企业大全
所在地址：	山东省济南市历城区七里河路12号腾峰园0-5
所属行业：	IT及数码-工业控制计算机及外围设备
邮政编码：	250100

Second address for Jinan Quanxin Fangyuan
Jinan Anchuang Information Technology Co. Ltd.

However, the website for Antorsoft, which was still active at the time of writing, names the company as 济南安创信息科技有限公司, which in English is rendered Jinan Anchuang Information Technology Co. Ltd. It claims to be a ‘state-level high-tech enterprise that integrates development, productions, management and technical services with scientific research as the guide’. It claims to ‘strive to become an excellent supplier of global information security services and communications products’.

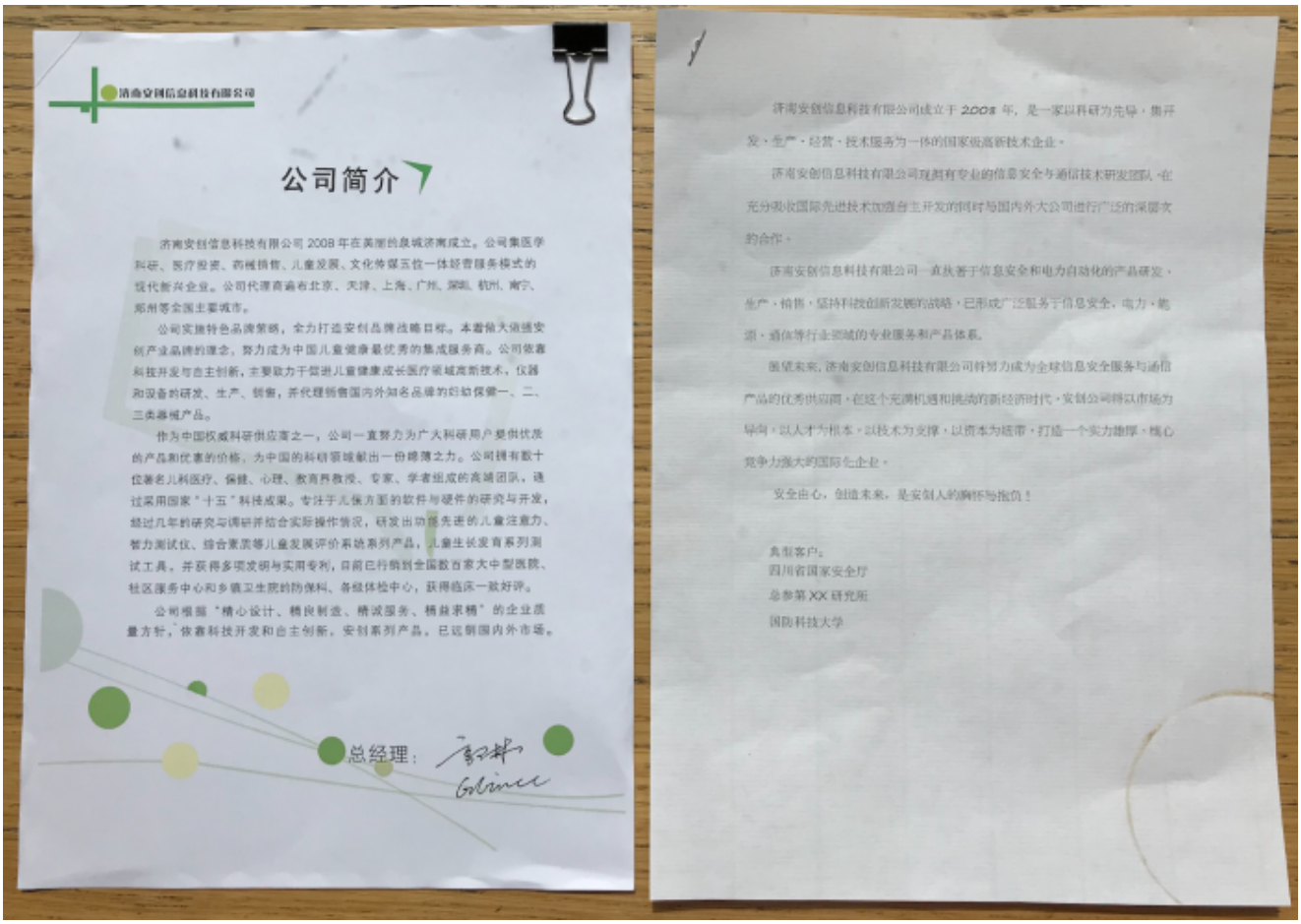
Antorsoft website showing Jinan Anchuang as the company name
On a second page Antorsoft claims to look at Cyber Security issues from the perspective of those committing Cyber attacks. What an interesting perspective to have chosen…

Antorsoft description of services offered

A healthcare company? With MSS links?

So far, so good. We've got a likely MSS Officer running and Information Technology company, or two, on the side. Why, then, in this brochure (left) – which we were passed by a friend – does Jinan Anchuang claim to be a healthcare company focusing on child health development? It is definitely the same company – you'll see that the brochure is signed by 郭林 (Guo Lin) using both his name and his 'Glince' nickname.

All becomes clear in a second version of the same document (right). No headed paper, no signature, but the same company name and founding date.



But. The description is different. Now it's an IT company. And at the bottom is a list of clients, including 四川省国家安全厅, the Sichuan State Security Department. For those not experts in Chinese national security departments, the SSSD is the provincial department of the Ministry of State Security in Sichuan.

Oops.

Sichuan isn't Shandong, where Jinan is located, but perhaps we will find more links later.

Use of alias names?

This is one of our favourite discoveries. Using (previously hacked and released) data from Chinese messaging service QQ, we were able to find Guo Lin's QQ account, which is 21213804. At the time that the data was released, 21213804 was a member of a number of QQ groups. In many of these, the name he used was 郭林, which is transliterated 'Guo Lin'. So far so good.

But the QQ data shows that he was also a member of an 'Antorsoft' group (QQ number 7043291) created in 2004. In that group he used the name 林子 (Lin Zi), Lin being his first (or 'given') name and Zi, in this instance, being used to extend a single syllable name into a nicer sounding two syllable word (Zi roughly translates to 'thing'). For the purposes of our analysis we will translate 'Zi' as 'Mr' – think Reservoir Dogs and you'll see why.

Looking at the other members of the Antorsoft group in the QQ data, a pattern begins to emerge. Each of them was a single name – some connected to their real name, some apparently random – with 'Zi' appended. In many cases, it seems to form a sort of nickname or 'codeword' – 林子, for example, means 'Mr Forest'. Here is the complete list:

- QQ 21213804 uses 'Mr Forest' 林子 (Linzi) in the Antorsoft group but normally uses the name 郭林 (Guo Lin)
- QQ 10832991 uses 'Mr Ocean' 海子 (Haizi) in the Antorsoft group but normally uses the names 龙海 (Long Hai) 'Dragon Ocean' and Fei Long (飞龙) 'Flying Dragon'
- QQ 23793808 uses 'Mr Bamboo' 竹子 (Zhuzi) in the Antorsoft group but also the name 'Zhuyuzi'
- QQ 87414156 uses 'Mr Monkey' 猴子 (Houzi) in the Antorsoft group
- QQ 369782831 uses 'Mr Pine' 松子 (Songzi) in the Antorsoft group
- QQ 1137938323 uses 亮子 (Liangzi) in the Antorsoft group
- QQ 26250040 uses 'Mr Chen' 陈子 (Chenzi) in the Antorsoft group but also the name 雨巷 (Yuxiang) or 'Rain Alley'

Interestingly, Yuxiang was also in a QQ group called 江苏公务员考试交流 (Jiangsu Civil Service Examination Exchange), created in 2009. The group description is the 南京大学公务员考试群 (Nanjing University Civil Service Examination Group), giving us another link to Nanjing.

In summary, we discovered two IT Security Companies based in Jinan, affiliated with a Chinese individual who studied Information Security to Masters level. Our source claims that individual is an active MSS Officer involved in Cyber operations. One of the companies appears to have some sort of healthcare company front, whilst simultaneously claiming to be an SSSD InfoSec contractor. And employees use alias names on QQ when dealing with Antorsoft.

What we still don't know is: who else works in these companies and do they have any connections to APT attacks?

#guoknowswherethisleads