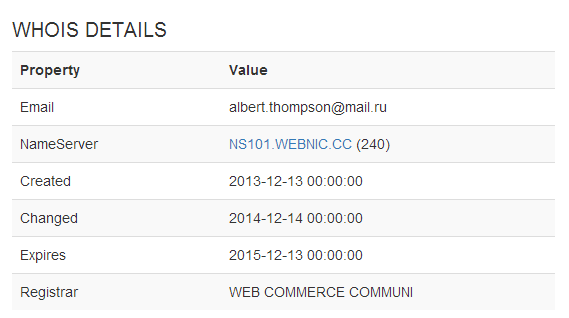
# 概述

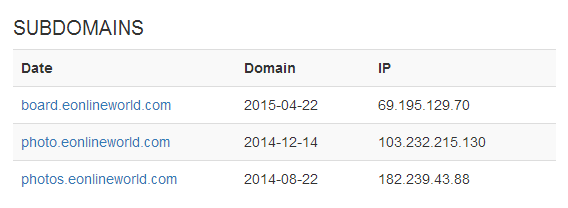
# 域名

域名的IP地址为69.195.129.72,该地址属于[乔·S数据中心有限责任公司](https://myip.ms/view/ip_owners/340274/Joe_S_Datacenter_LLC.html)，邮箱地址为albert.thompson@mail.ru

域名网址：

<https://www.threatcrowd.org/domain.php?domain=photo.eonlineworld.com>

子域信息



PORT(端口)80

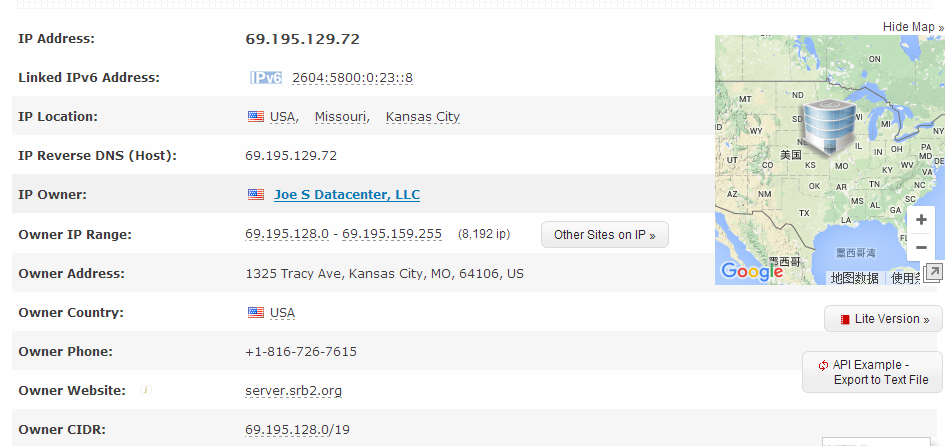
|  |
| --- |
| HTTP/1.1 301 Moved Permanently  Server: Tengine/1.4.2  Date: Tue, 06 Jan 2015 07:42:22 GMT  Content-Type: text/html  Content-Length: 286  Connection: keep-alive  Location: http://173.245.86.201/  [!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">  [html>  [head>[title>301 Moved Permanently[/title>[/head>  [body bgcolor="white">  [h1>301 Moved Permanently[/h1>  [p>The requested resource has been assigned a new permanent URI.[/p>  [hr/>Powered by Tengine/1.4.2  [/body>  [/html> |

信息来源：

<https://www.threatcrowd.org/domain.php?domain=photo.eonlineworld.com>

文档信息链接：

<https://securelist.com/files/2014/11/darkhotelappendixindicators_kl.pdf>



信息来源：

<https://myip.ms/info/whois/69.195.129.72>

截止到2016年3月底反钓鱼公司PhishMe观察到93%的网络钓鱼电子邮件包含Ransomware，PhishMe公司报道的新闻说2016年第一季度观察到整个网络的钓鱼邮件已达到630万，比2015年同期增长了789%，PhishMe公司的专家介绍所有恶意消息中的51%被用来传播Ransomware。Ransomware正在成为一个享有特权的网络罪犯迅速赚钱的工具,这种类型的威胁正在改变的扩散威胁景观场景中

信息来源：

<http://securityaffairs.co/wordpress/48099/hacking/phishing-ransomware.html>

## 利用旅馆WiFi窃取高管隐私数据

黑客实施攻击会在高管办理完入住手续，并连接到旅馆WiFi网络，提交房号和姓氏登陆之后。攻击者在看到高管连接到受感染的网络之后，将木马跟随用户的下载文件安装到设备上，假装是某款受信任应用（比如Google Toolbar, Adobe Flash或者Windows Messenger）的更新在用户设备上植入后门，然后设备就会感染。”

信息来源：

<http://www.cnbeta.com/articles/344989.htm>

