

威胁情报分析实战

薛锋 微步在线

提纲

- 微步在线简介
- 威胁情报理解
- TI兵器库之子域名
- TI兵器库之历史IP
- TI兵器库之历史Whois
- 案例

微步在线 - 国内首家专业威胁情报公司

#威胁情报

#安全 #威胁分析 #SaaS #大数据 #AI

威胁情报分析

数据 + 分析

子域名 - 0ops.net

- 9个

0con.0ops.net: 0

blog.0ops.net: 0

ctf.0ops.net: 0

dl.0ops.net: 0

ftp.0ops.net: 0

pantologic.0ops.net: 0

war.0ops.net: 0

wiki.0ops.net: 0

www.0ops.net: 0

子域名 - jd.com

- 21286

aolando.jd.com: 0

aoleyuan.jd.com: 0

aoliang.jd.com: 0

ipr.360buy.jd.com: 0

l.activity.jd.com: 0

ls.activity.jd.com: 0

m.activity.jd.com: 0

recommend.ado.jd.com: 0

www.11th.jd.com: 0

www.8th.jd.com: 0

www.9377.jd.com: 0

.....

子域名总结

- 资产管理
- 漏洞扫描
- 关联分析



历史IP - 0ops.net






- 0ops.net

IP地址	
IP地址	127.0.0.1 (共有 1000+ 个域名指向此地址)
地理位置	本机地址,本机地址
ASN	无ASN信息

历史解析记录			
时间	IP	国家	省 / 州
2014-10-13	127.0.0.1	本机地址	本机地址
2014-02-23	202.120.7.22	中国	上海
2012-09-11	208.43.167.112	美国	华盛顿州
2011-09-22	174.120.203.2	美国	德克萨斯州

历史IP - Google.com

IP地址	
IP地址	106.162.192.148 (共有 0 个域名指向此地址) 
地理位置	日本,日本
ASN	2516 (KDDI KDDI CORPORATION, JP) 低风险 

历史解析记录			
时间	IP	国家	省 / 州
2016-04-18	106.162.192.148 	日本	日本
2016-04-17	101.96.118.102 	越南	越南
2016-04-16	108.177.14.100 	美国	美国
2016-04-15	106.162.216.103 	日本	日本
2016-04-14	108.177.15.100 	美国	美国
		991 显示更多	

Whois历史 - netforuser.com

当前注册信息	
注册者	Spy Eye (相关域名 500+ 个)
注册机构	
邮箱	the.malware.cabal@gmail.com (相关域名 500+ 个)

2014-03-27	<div>修改：</div> <div>电话: 8605922577888 → 01066569215</div> <div>注册者: Whois Agent → Zhong Si</div> <div>注册机构: Whois Privacy Protection Service → Xicheng Co.</div> <div>邮箱: gmvjcxkxhs@whoisservices.cn → ctouma2@googlemail.com</div>
------------	--

IP反解域名

指向同一IP的域名列表	
域名	域名
powerswimohave.at	www.powerswimohave.at
aiqirjaoisjghqwhjsagjos.biz	www.aiqirjaoisjghqwhjsagjos.biz
akamosyter.biz	www.akamosyter.biz
asdfnomore87salesh.biz	www.asdfnomore87salesh.biz
bank-manager.biz	www.bank-manager.biz
1000 显示更多	

案例 - XCodeGhost

- init.icloud-analysis.com

52.2.85.22 IP信息	
IP地址	52.2.85.22 (共有 0 个域名共用此地址)
地理位置	美国,弗吉尼亚州,阿什本
ASN	14618 (AMAZON-AES - Amazon.com, Inc., US) 中风险 ?

2015-09-21		×
注册者	Registration Private	
注册机构	Domains By Proxy, LLC	
邮箱	ICLOUD-ANALYSIS.COM@domainsbyproxy.com	
地址		
电话	+1.4806242599	
注册时间	2015-02-25 00:00:00	
过期时间	2016-02-25 00:00:00	
更新时间	2015-02-25 00:00:00	
域名服务商	GoDaddy.com, LLC	
域名服务器	ns35.domaincontrol.com; ns36.domaincontrol.com	

案例 - XCodeGhost - 历史IP

- init.icloud-analysis.com

历史解析记录			
时间	IP	国家	省 / 州
2016-03-18	178.162.203.202 	德国	黑森州
2016-03-12	213.165.83.176 	德国	德国
2015-12-15	50.21.181.152	美国	堪萨斯州
2015-11-02	213.165.83.176 	德国	德国
2015-10-16	50.21.181.152	美国	堪萨斯州
2015-10-05	74.208.153.9	美国	堪萨斯州
2015-10-04	213.165.83.176 	德国	德国
2015-08-27	52.2.85.22 	美国	弗吉尼亚州
2015-08-08	52.2.85.22 	美国	弗吉尼亚州
2015-07-21	52.2.85.22	美国	弗吉尼亚州
2015-05-20	52.4.74.88 	美国	弗吉尼亚州
2015-05-11	52.4.74.88	美国	弗吉尼亚州
2015-03-20	104.238.125.92	美国	亚利桑那州
2015-03-04	52.10.173.198	美国	俄勒冈州
2015-03-03	182.92.101.29 	中国	北京
2015-02-26	50.63.202.48	美国	亚利桑那州

案例 - XCodeGhost - IP反查

2shoubang.com 分析报告

域名服务商 XINNET TECHNOLOGY CORPORATION
域名服务器 f1g1ns1.dnspod.net; f1g1ns2.dnspod.net
Alex排名 N/A

威胁情报

IP分析

Whois

可视分析

IP地址

IP地址 52.5.46.89 (共有 0 个域名指向此地址)

地理位置 美国,弗吉尼亚州,阿什本

ASN 14618 (AMAZON-AES - Amazon.com, Inc., US) 中风险 ?

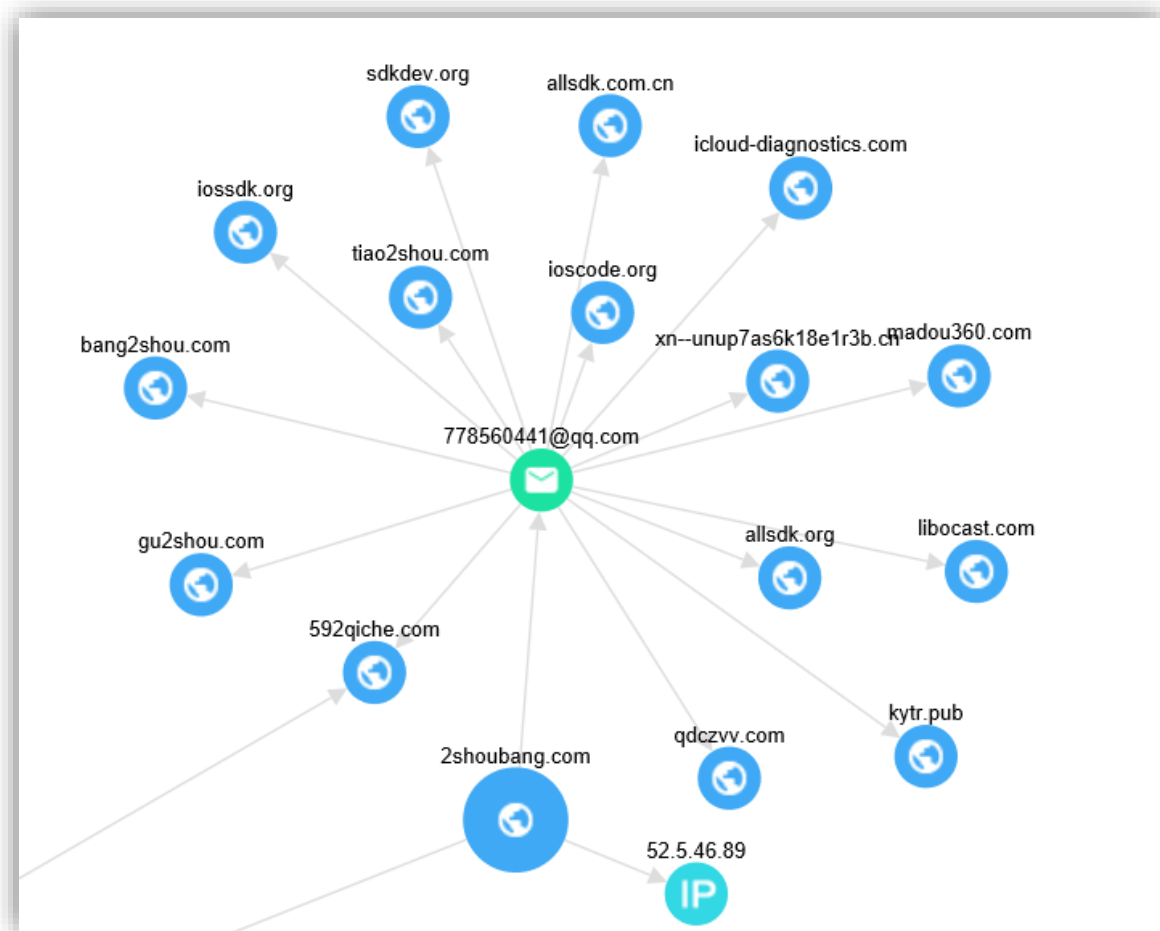
历史解析记录

时间	IP	国家	省 / 州
2015-07-02	52.5.46.89	美国	弗吉尼亚州
2015-03-18	182.92.101.29	中国	北京

案例 - XCodeGhost - Whois

2015-09-01		×
注册者	wang long	
注册机构	wang long	
邮箱	778560441@qq.com	
地址		
电话	0860537 55580507	
注册时间	2014-10-07 00:00:00	
过期时间	2015-10-07 00:00:00	
更新时间	2015-07-01 00:00:00	
域名服务商	XIN NET TECHNOLOGY CORPORATION	
域名服务器	f1g1ns1.dnspod.net; f1g1ns2.dnspod.net	
		关闭

案例 - XCodeGhost - Email反查



案例 – XCodeGhost – SDKdev.org

2015-06-01 ×

注册者	long wang
注册机构	
邮箱	778560441@qq.com
地址	
电话	+86.13276422520
注册时间	2015-04-07 00:00:00
过期时间	2016-04-07 00:00:00
更新时间	2015-04-07 00:00:00
域名服务商	GoDaddy.com, LLC (R91-LROR)
域名服务器	ns67.domaincontrol.com; ns68.domaincontrol.com

关闭



谢谢

www.VirusBook.cn