Botnet

僵尸网络911 S5的数字遗产

lvxing
Jun 14, 2024 • 7 min read

概述

2024年5月29日，美国司法部发布通告，声称其执法活动摧毁了"史上最大的僵尸网络" 911 S5，查封了相关域名，并且逮捕了其管理员YunHe Wang。Wang及其同伙通过创建并分发包含恶意代码的免费VPN程序感染用户，并且在名为911 S5的住宅代理服务中出售对被感染设备构成的代理网络的访问权。

按照360威胁情报中心的分析，911S5从2014年开始运营，到2022年7月关停，在2023年10月又摇身一变，化名CloudRouter继续其肮脏生意，终于在2024年5月被多国联合执法摧毁。911S5的僵尸网络运行时间长、涉及多个国家的19M个IP地址、行为高调，虽然经过执法行动后大势已去，但是其数字遗产仍然对网络空间构成了现实且显著的威胁，下文是我们对威胁分析的结果。

"空手套白狼"的911 S5

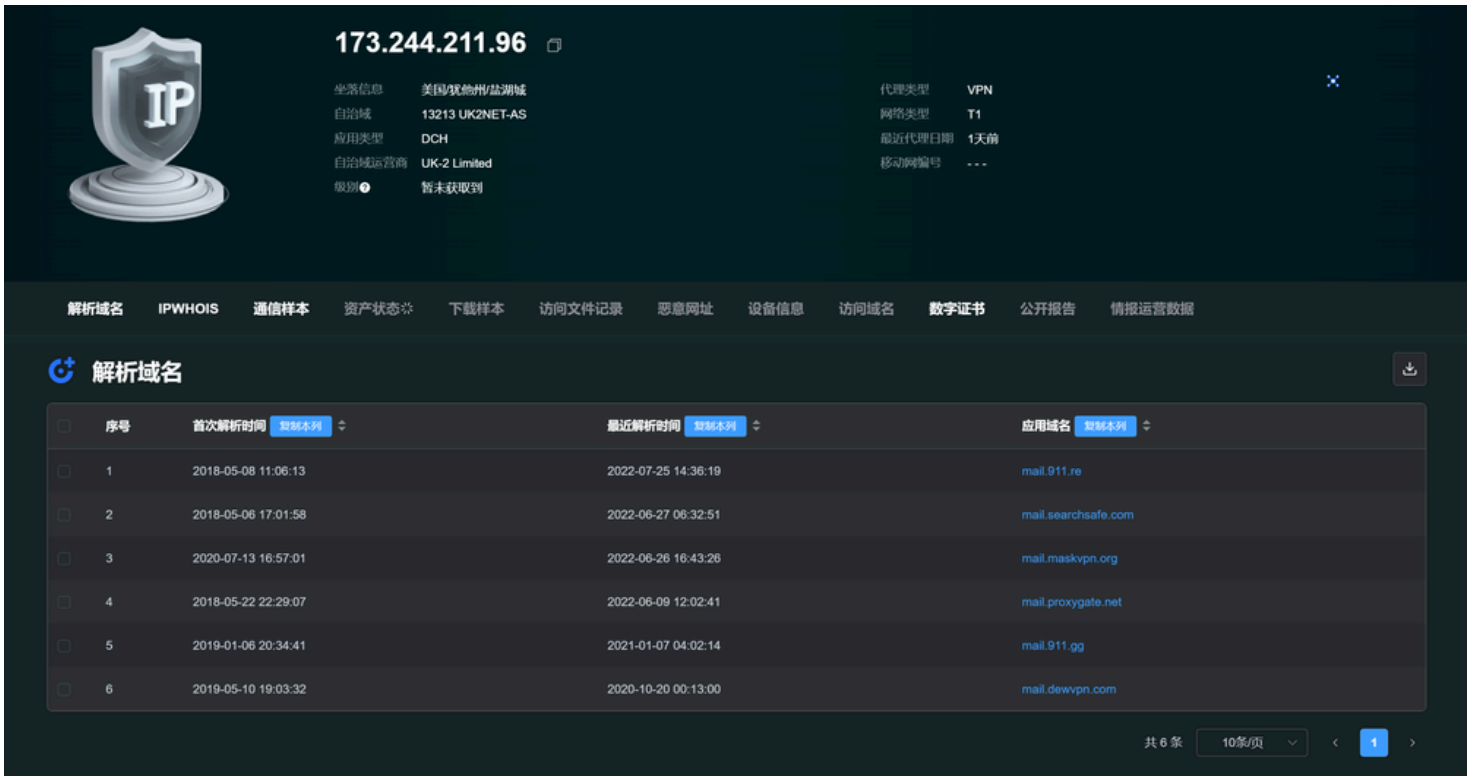
911S5出售的代理服务背后是数千万被感染的设备。受害者主动或被动下载捆绑了恶意代码的软件、免费VPN程序等。在程序启动后，恶意代码将会创建持久化服务作为后门，为911S5客户提供代理服务。

在2023年以前，911S5使用的免费VPN包括:ProxyGate、MaskVPN、DewVPN与ShineVPN。我们观察到最早出现的VPN程序是ProxyGate，在2016年至2020年间活跃。

911S5与VPN程序的强关联

共同的基础设施

将911S5与一众免费VPN关联起来的关键性证据就是它们共用了一部分基础设施。我们注意到，`911.re`、`searchsafe.com`、`maskvpn.org`、`proxygate`、`911.gg`、`dewvpn.com`的电子邮件服务都曾被解析到同一个服务器:`173.244.211.96`，证明911S5和特定免费VPN程序拥有共同的运营者。



更多数据，请查看最后一部分"共用IP"。

相似的样本行为

MaskVPN、DewVPN以及ShineVPN拥有相似的编码方式、进程链结构:

MaskVPN进程链

DewVPN进程链

“死而复生”的CloudRouter

2022年7月，911S5的运营者停止了911S5的服务，但是它们也并未蛰伏太长时间。2023年2月，911S5的继任者CloudRouter被研究人员发现；10月，CloudRouter正

式发布，提供类似911S5的住宅服务，它使用PaladinVPN、Shield VPN感染设备并继续构建代理网络，我们确认这是换汤不换药的911S5。

CloudRouter，换汤不换药

共用基础设施

与911S5类似，`cloudrouter.pro`、`paladinvpn.com`、`shieldvpn.org`的电子邮件服务解析到了相同的服务器:`209.126.108.53`。

更多数据，请查看最后一部分"共用IP"。

样本的强关联

1. CloudRouter使用的PaladinVPN、ShineVPN的编码方式、进程链与MaskVPN、DewVPN高度相似。

PaladinVPN进程链

2. 根据美国法院的扣押文件，在2023年8月份，分析人员观察到了从MaskVPN到ShieldVPN的升级，该文件声称ShieldVPN、PaladinVPN与 `reachfresh.com` 通信，并从 `updatepanel.cc` & `upgradeportal.org` 接受更新指令。

PaladinVPN的推广域名

我们注意到，有150+个推广域名都解析到了同一个地址 `148.72.152.203` ，如：

```
soccerstreamingvpn.com
freevpnlebanon.com
freevpnhongkong.com
freevpncuba.com
freevpnghana.com
```

这些站点的内容诱导访问者前往PaladinVPN相关的页面。美国法院的一份扣押文件声称，它们确定这是由Wang的一名同谋所为。

域名热度

我们分析了911S5相关域名的热度并绘制了折线图，其中纵轴表示热度值，范围为[0,10]，横轴表示时间。

域名热度折线图

容易发现，大部分域名的热度值在[2,4]，`911.re`、`911s5.com`两个域名热度较高，`911.re`在热度最高时接近6。

IOC

域名

```
proxygate.net
911s5.net
911.re
911.gg
911s5.org
911s5.com
maskvpn.cc
maskvpn.org
dewvpn.cc
dewvpn.com
dewvpn.net
dewvpn.org
shinevpn.org
```

```
shinevpn.com
shinevpn.co
shinevpn.net
cloudrouting.net
cloudrouter.io
cloudrouter.pro
paladinvpn.org
paladinvpn.com
shieldvpn.org
reachfresh.com
updatepanel.cc
upgradeportal.org
```

下载域名与URL

```
dton09jc5wlle.cloudfront.net
d2mxl8paokc6p3.cloudfront.net
d32cjgd79n340u.cloudfront.net
https://d87hw114pqw7b.cloudfront.net/dewvpn-setup.exe
https://d3d5qtzjda7oy3.cloudfront.net/paladinvpn-setup.exe
https://d2akdl6qfujxx9.cloudfront.net/paladinvpn-setup.exe
https://d1f64skmkl5mzn.cloudfront.net/paladinvpn.exe
https://d2akdl6qfujxx9.cloudfront.net/paladinvpn-setup.exe
https://d1f64skmkl5mzn.cloudfront.net/paladinvpn.exe
https://dton09jc5w11e.cloudfront.net/paladinvpn.exe
```

样本

```
1875e43e224862cbf60bffc51c96cf1a
25e627a9a583f08ffbbd60cbc276f87e
3a6995457c832ecf79be7b941bfa4d91
3e68dbd53c2df48e00f830243b35cd84
3f056ee26ac0a3d3bf0bb4570887c925
```

PaladinVPN

```
6db6b7b99a0e87f142a56e256a62ef82
fd72d909e280110cd6ccbae8e86d29e4
fc8fcf280914e20c93939ed155a68c53
026dc4084820a013ec1537ba6bab0d44
d6d577fc72559cfb133b4c02c21dc7c0
```

ShieldVPN

共用IP

借助360威胁情报数据库，我们找到了一批911S5不同域名共用的IP地址：

```
34.102.136.180
        911s5.net
        911s5.org
        maskvpn.org
        shinevpn.org
        shinevpn.com
        shinevpn.net
34.98.99.30
        911s5.org
        911s5.com
        dewvpn.org
        dewvpn.net
        dewvpn.cc
        maskvpn.cc
        maskvpn.org
        proxygate.net
174.139.8.2
        911s5.org
        911s5.com
        www.911s5.com
        eu.911.gg
        911.re
        login.911s5.net
        userip.911s5.net
        neibu.911s5.net
31.13.83.2
        eu.911.gg
        www.911.gg
        911.gg
        www.dewvpn.com
        dewvpn.com
        net.dewvpn.com
31.13.84.2
        eu.911.gg
        www.911.gg
        911.gg
        www.dewvpn.com
        user.dewvpn.com
        net.dewvpn.com
31.13.106.4
        eu.911.gg
        dewvpn.com
98.126.28.10
        911s5.org
        www.911s5.com
```

911s5.com
185.45.6.57
eu.911.gg
user.dewvpn.com
www.dewvpn.com
31.13.73.9
eu.911.gg
911.gg
www.911.gg
www.dewvpn.com
user.dewvpn.com
net.dewvpn.com
162.125.8.1
eu.911.gg
www.911.gg
911.gg
dewvpn.com
www.dewvpn.com
user.dewvpn.com
net.dewvpn.com
31.13.92.5
www.911.gg
eu.911.gg
911.gg
dewvpn.com
www.dewvpn.com
net.dewvpn.com
162.125.2.3
eu.911.gg
911.gg
www.911.gg
dewvpn.com
www.dewvpn.com
net.dewvpn.com
185.45.7.97
eu.911.gg
www.dewvpn.com
162.125.2.5
eu.911.gg
www.911.gg
911.gg
dewvpn.com
user.dewvpn.com
www.dewvpn.com
net.dewvpn.com
31.13.64.7
eu.911.gg
www.911.gg
911.gg
www.dewvpn.com
user.dewvpn.com
net.dewvpn.com
31.13.74.1

```
        eu.911.gg
        www.911.gg
        911.gg
        user.dewvpn.com
        www.dewvpn.com
        net.dewvpn.com
31.13.69.86
        eu.911.gg
        dewvpn.com
31.13.67.33
        eu.911.gg
        dewvpn.com
        user.dewvpn.com
31.13.94.7
        eu.911.gg
        911.gg
        www.911.gg
        www.dewvpn.com
        user.dewvpn.com
        net.dewvpn.com
31.13.70.33
        eu.911.gg
        user.dewvpn.com
31.13.70.13
        eu.911.gg
        dewvpn.com
        user.dewvpn.com
31.13.80.1
        eu.911.gg
        www.911.gg
        911.gg
        www.dewvpn.com
        net.dewvpn.com
162.125.7.1
        eu.911.gg
        www.911.gg
        911.gg
        user.dewvpn.com
        net.dewvpn.com
103.97.3.19
        www.911.gg
        911.gg
        dewvpn.com
        www.dewvpn.com
        net.dewvpn.com
31.13.75.12
        eu.911.gg
        user.dewvpn.com
162.125.6.1
        eu.911.gg
        911.gg
        www.911.gg
        user.dewvpn.com
```

```
        www.dewvpn.com
        net.dewvpn.com
31.13.71.19
        eu.911.gg
        user.dewvpn.com
31.13.81.4
        eu.911.gg
        911.gg
        www.911.gg
        www.dewvpn.com
        net.dewvpn.com
162.125.1.8
        eu.911.gg
        www.911.gg
        911.gg
        www.dewvpn.com
        net.dewvpn.com
31.13.75.5
        eu.911.gg
        911.gg
        www.911.gg
        www.dewvpn.com
        user.dewvpn.com
        net.dewvpn.com
31.13.84.8
        eu.911.gg
        www.911.gg
        911.gg
        user.dewvpn.com
        www.dewvpn.com
        net.dewvpn.com
31.13.69.33
        eu.911.gg
        user.dewvpn.com
        dewvpn.com
31.13.84.1
        eu.911.gg
        www.911.gg
        911.gg
        user.dewvpn.com
        www.dewvpn.com
        net.dewvpn.com
157.240.3.8
        eu.911.gg
        www.911.gg
        911.gg
        www.dewvpn.com
        dewvpn.com
        net.dewvpn.com
```

— 360 Netlab Blog - Network Security Research Lab at 360 —

Botnet

Botnet

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

Overview On Oct 21, 2022, 360Netlab's honeypot system captured a suspicious ELF file ee07a74d12c0bb3594965b51d0e45b6f, which propagated via F5 vulnerability with zero VT detection, our system observces that it communicates with IP 45.9.150.144 using SSL with forged Kaspersky certificates, this caught our attention....

Jan 10, 2023 · 13 min read