

MuddyWater组织近期钓鱼攻击活动分析 | CTF导航

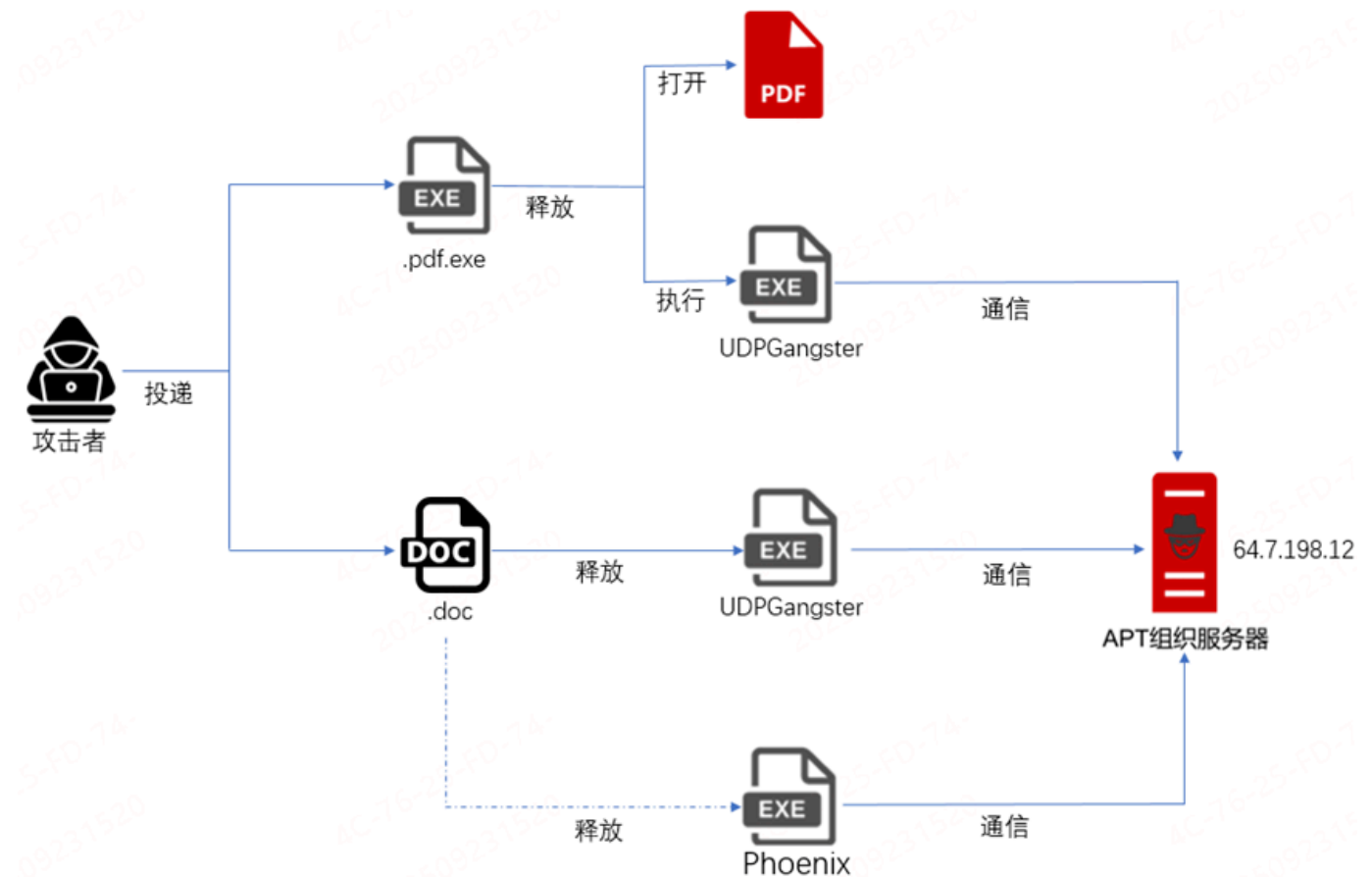
ctfiot.com/282122.html

MuddyWater（又称Static Kitten或MERCURY）是一个疑似由伊朗政府支持的APT（高级持续性威胁）组织，其活动最早可追溯至2017年初。该组织主要活跃于中东地区，同时也针对欧洲和北美国家发动攻击，目标行业包括政府机构、军事组织、电信企业及石油公司等。MuddyWater组织以鱼叉式网络钓鱼攻击著称，其攻击手法高度隐蔽，善于利用多种攻击载荷，并不断更新攻击载荷，以维持攻击效果和规避防御。近日360高级威胁研究院捕获到MuddyWater组织针对多个地区发起的多起网络攻击活动。该组织在攻击中采用宏代码和伪装为PDF文件的可执行程序投递恶意载荷，最终释放UDPGangster后门，并同步部署Phoenix后门进行窃密行动。值得注意的是，MuddyWater已逐渐减少使用RMM等现成远控程序，转而开发并部署多种专用后门以针对特定目标实施渗透。为帮助企业与个人了解其攻击链条并强化防护，本报告将对其近期的攻击活动与载荷特征进行深入分析与披露。

一、攻击活动分析

1. 攻击流程分析

本次攻击中，MuddyWater组织通过投递伪装成PDF的可执行文件以及携带宏代码的DOC文件进行钓鱼攻击，恶意文件一旦被打开，便会释放UDPGangster后门进行窃密行动，与此同时我们也关联到与之相同C2的Phoenix后门（该类型在之前行动中通过宏代码释放），整个攻击流程如下图所示：



2. 攻击载荷分析

我们捕获到MuddyWater组织分别使用伪装成PDF的可执行文件以及携带宏代码的DOC文件，来进行投递UDPGangster后门的攻击载荷，MuddyWater组织攻击使用这两种不同的载荷投递方法，展现了该组织攻击手法的多样性。我们依次展开分析。

1) 伪装成PDF文件的载荷分析

样本具体信息如下：

MD5 bed77abc7e12230439c0b53dd68ffaf7

文件名称 Transfer receipt#27789.pdf .exe

文件大小 2.30 MB (2,417,152 字节)

编译时间 2025-08-12 18:57:52

“Transfer receipt#27789.pdf .exe”是一个伪装成PDF文档的可执行文件，文件图标也使用PDF文档图标，用于迷惑受害者。

该程序主要功能是释放伪装文件，并加载shellcode。一旦该程序执行，首先会将自身携带的伪装文档释放到当前目录下。

伪装文档是一份以色列公司Cardinal Tours Ltd的收据或付款凭证，使用的语言为希伯来语，该语种为以色列官方语言之一。

然后使用Base64编码结合循环右移解密自身携带的最终攻击载荷，最后通过内存装载的方式执行最终载荷。

其加载的最终载荷信息如下：

MD5 de14abbda6a649d9ec90a816847f95db

文件大小 675 KB (691,712 字节)

编译时间 2025-08-12 17:43:52

PDB路径 C:\Users\gangstersource\repos\udp_3.0 - Copy\64\release_86\udp_3.0.pdb

该载荷是一个被称为UDPGangster的后门程序，该后门命名是根据PDB路径中的gangster和udp_3.0结合而来。UDPGangster是一个后门程序，首先它会将自身复制到“C:\Users\[username]\AppData\Roaming\Low\SystemProc.exe”，然后通过写入注册表“Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup”实现自启动。

接着试图读取位于“C:\Users\[username]\AppData\Local\Locala27af8cada0fc6e752338f0194t8k56e024169fe98a44190259ede0ae4d75ef4”的C2配置文件，如果读取失败，则会使用硬编码的C2地址（64.7.198.12）

然后收集主机名，工作组，操作系统版本和用户名等信息，加密后发送给服务端。

最后从C2服务端接收指令，然后执行不同的功能，完成对目标用户主机的远程控制。

UDPGangster目前是一个功能较简单的后门程序，具体功能如下：

命令号	功能
4	系统休眠
10	创建shell并执行命令
20	搜集文件并外传至C2服务器
30	向受害者机器下发恶意文件
99	从远端接收C2配置文件

2) 宏样本分析

攻击者除了使用伪装成PDF文件的载荷外，还使用了携带恶意宏代码的DOC文件，下面是其中一个样本的基本信息：

MD5	561b2983d558283c446ff674ff6138c3
文件名称	Transfer receipt#27790.doc
文件大小	3.83 MB (4,021,248 字节)

该文档是一个携带恶意宏代码的DOC文件，其释放的伪装文件与上述分析的”Transfer receipt#27789.pdf.exe” 样本具有相似性，但部分内容被刻意遮盖。

值得注意的是，其他同类恶意宏样本通常会释放未经遮盖的完整伪装文件，如下图所示,这表明攻击者可能针对不同目标采用了差异化的伪装内容。

一旦打开这类恶意文档，就会后台静默执行宏代码，该文件宏代码首先从文档自身解密释放后续载荷到“C:\Users\Public\Downloads\novaservice.txt”，然后重命名为“C:\Users\Public\Downloads\novaservice.exe”，最后执行novaservice.exe。

其释放的novaservice.exe信息如下：

MD5 7bfb76c7eeb652d73b85c99ee83b339

文件名称 novaservice.exe

文件大小 1.81 MB (1,902,080 字节)

编译时间 2025-08-11 14:16:23

“novaservice.exe”和“Transfer receipt#27789.pdf.exe”功能是相近，都是内存装载UDPGangster后门的装载器。区别在于“Transfer receipt#27789.pdf.exe”会释放伪装内容，而“novaservice.exe”只是内存装载UDPGangster后门，不再释放伪装内容。

“novaservice.exe”内存装载的UDPGangster后门信息如下：

MD5 d84812961fc7cd8340031efd7b5508a8

文件大小 676 KB (692,224 字节)

编译时间 2025-08-09 21:27:21

PDB路径 C:\Users\gangstersource\repos\udp_3.0 - Copy\64\release_86\udp_3.0.pdb

经过分析，“Transfer receipt#27790.doc”最终内存装载的UDPGangster后门和“Transfer receipt#27789.pdf.exe”装载的UDPGangster后门差别不大，唯一的差别在于前者使用powershell mv命令移动自身文件，而后者使用MoveFileA函数移动自身文件。

二、关联分析

根据上面分析的C2: 64.7.198.12我们关联到另一个样本，该样本属于Phoenix后门，其信息如下所示：

MD5 a546d2363a4b94e361d0874b690c853b

文件名称 71csc2c.exe

文件大小 837 KB (857088 字节)

编译时间 2025-08-14 15:13:16 UTC

样本执行时，首先使用CryptStringToBinaryA将Base64字符串转为二进制，接着对每个字节执行4次减法：(((byte - 2) - 6) - 8) - 10得到payload,最后在当前进程空间中执行解密后的payload。

Payload被加载起来时候，首先创建互斥体“gtfo”，然后获取公网IP地址。

接着获取计算机名、用户名和操作系统版本等信息采用post的方式将收集的信息送到服务器。

然后等待服务器响应执行下一步指令，具体指令如下：

相关指令信息如下，与Phoenix后门组件的特征行为完全吻合，此外，C2通信模式也一致。

指令	描述
cmd	执行shell
Upload	文件上传
timeout	设置超时时间
Persisit	持久化

三、归属研判

通过对MuddyWater组织攻击活动的相关信息进行深入分析，发现此次披露的载荷攻击符合该组织以往的TTP，具体表现如下：

1. 通过对这两类组件的详细分析，发现与MuddyWater组织去年常用的BugSleep存在显著相似性，例如加载器中字符串解密均采用每个字节减去硬编码数字的算法，且最终恶意组件的远控命令高度重合（包括上传文件、执行shell、设置超时时间及创建持久化任务等）。这些高度一致的代码逻辑和功能设计进一步佐证了这类组件与MuddyWater组织的关联性，符合该组织长期以来的攻击工具开发模式。具体可参考CheckPoint发布的分析文章[1]。
2. 通过对C2服务器（64.7.198.12）的威胁情报关联分析，确认Phoenix与UDPGangster两类恶意载荷均与其建立通信连接，且溯源分析显示其样本特征及基础设施特征与Group-IB公司披露的MuddyWater组织攻击框架[2]吻合，该报告明确将这两类组件归因于MuddyWater组织，进一步证实了这些恶意载荷的同源性及其与APT组织的强关联性。
3. 本次MuddyWater组织使用的宏代码执行流程与之前的样本也类似，都是利用Document_Open事件在文档打开时自动执行，从隐藏在表单中的编码数据中解密出恶意二进制文件，写入并重命名到指定路径后再调用系统命令（如Shell或ShellExecute）执行。此外，在解密二进制文件的算法上也与早期样本表现一致，均是通过减偏移→模256→转字符的方式。
4. 样本的伪装内容为以色列语言和阿塞拜疆语言及英语，并且样本也由以色列和阿塞拜疆等地区上传，符合MuddyWater组织的攻击目标。

综上，我们将这类攻击归属于MuddyWater组织。

总结

MuddyWater组织近年来持续保持高度活跃态势，但其攻击策略在2025年出现显著演变：该组织逐步减少对远程管理工具（RMM）的依赖，转而通过宏代码和伪装为PDF的可执行文件投递各类木马，其中Phoenix与UDPGangster后门程序成为其近期攻击活动的典型代表。本文通过分析相关样本的代码特征、行为模式及攻

击传播链条，旨在帮助用户全面了解其攻击路径与技术手法。此外需要特别强调的是，面对此类不断演变的定向攻击，各类组织机构及个人用户需强化安全意识，对可疑邮件附件、非可信来源的压缩文件及诱导性链接保持高度警惕，以免中招。

附录 IOC

MD5

bed77abc7e12230439c0b53dd68ffaf7
de14abbda6a649d9ec90a816847f95db
561b2983d558283c446ff674ff6138c3
7bfb76c7eeb652d73b85c99ee83b339
07502104c6884e6151f6e0a53966e199
aa75a0baebc93d4ca7498453ef64128a
409d02d6153af220e527fd72256ee3a5
a546d2363a4b94e361d0874b690c853b
9e06b36f4da737b8d699a6846c2540e9
e09a720574a6594b1444ebc1d6cca969
d84812961fc7cd8340031efd7b5508a8
dd6af28d1a03193fc76001b04d5827cc
a39f74247367e0891f18b7662c8e69b5
e5dd608292b6f421b0c108816d25fc5e
a9235540208fa6a25614c24a59e19199

C2

http[:]//64.7.198[.]12:8080/request
http[:]//64.7.198[.]12:8080/register
http[:]//64.7.198[.]12:8080/imalive
64.7.198[.]12:1259
157.20.182[.]75:1269

参考

[1]<https://research.checkpoint.com/2024/new-bugsleep-backdoor-deployed-in-recent-muddywater-campaigns/>

[2]<https://www.group-ib.com/blog/muddywater-infrastructure-malware/#introduction>

团队介绍

TEAM INTRODUCTION

360高级威胁研究院

360高级威胁研究院是360政企安全集团的核心能力支持部门，由360资深安全专家组成，专注于高级威胁的发现、防御、处置和研究，曾在全球范围内率先捕获双杀、双星、噩梦公式等多起业界知名的0day在野攻击，独家披露多个国家级APT组织的高级行动，赢得业内外广泛认可，为360保障国家网络安全提供有力支撑。

| 本篇文章来源于微信公众号: 360威胁情报中心