警惕APT-C-01（毒云藤）组织的钓鱼攻击

原创 高级威胁研究院 360威胁情报中心 2024年11月29日 17:18 北京

APT-C-01

毒云藤

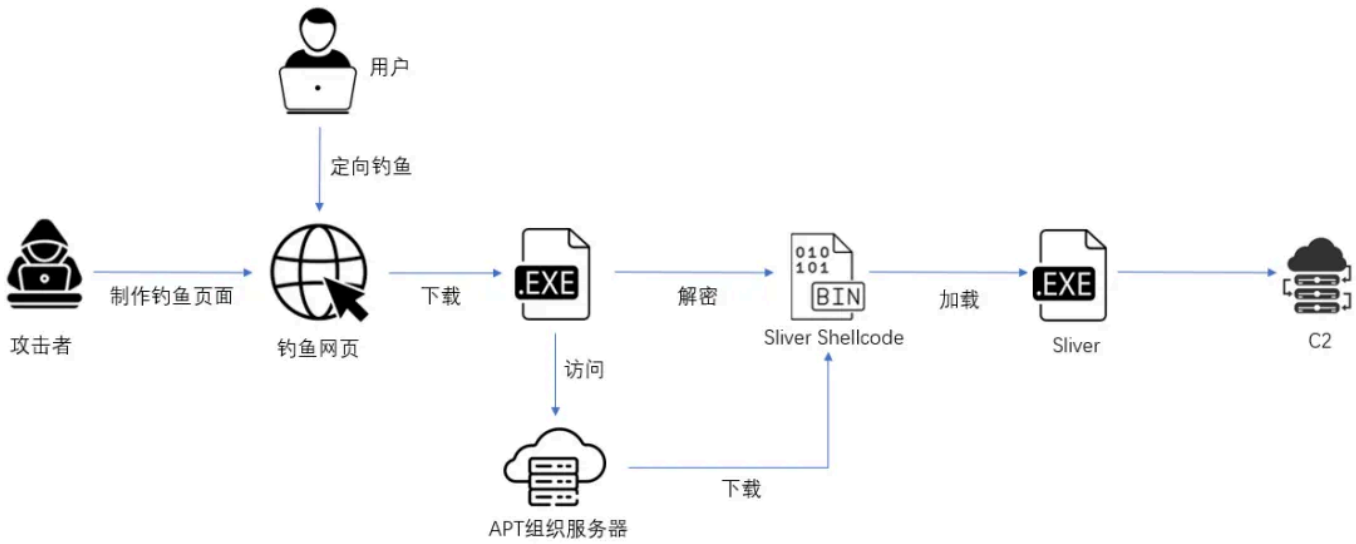
APT-C-01（毒云藤），是一个专门针对国防、政府、科技和教育等领域进行持续网络攻击的APT组织，活动已持续多年，起源可追溯至2007年。该组织惯用钓鱼攻击，包括水坑钓鱼、鱼叉式钓鱼，这些攻击手法往往针对特定目标，利用个性化的诱饵内容，以提高成功率。

近期我们在日常威胁狩猎中观察到该组织持续活动，其模仿官方网站制作钓鱼网页进行定向钓鱼，当受害者访问这类网站时会自动下恶意载荷，该载荷会进一步加载Sliver RAT进行窃密和远程控制行动。鉴于此，我们披露整个攻击流程，以便用户及时发现，避免中招。

攻击活动分析

1.攻击流程分析

毒云藤组织擅于模仿官方网站精心制作钓鱼页面，当目标群体打开这类网站时，会自动下载恶意载荷，该载荷是一个由C#编写的加载器，执行时会下载数据文件并进行解密出Shellcode再加载，Shellcode加载最终的Sliver RAT。整个流程如下图所示：



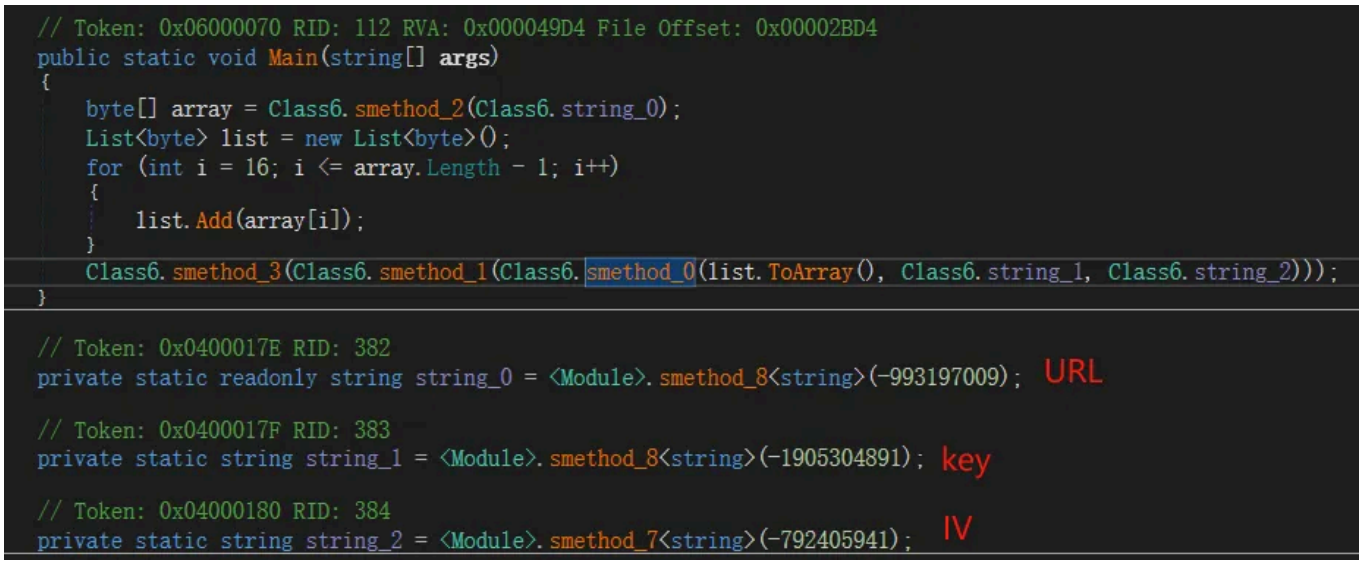
2.恶意载荷分析

我们捕获了多个恶意加载器样本，这些加载器都使用PDF图标来伪装以此迷惑受害者，以其中一个进行分析，如下所示。

MD5	61c42751f6bb4efafec524be23055fba
文件名称	auto-download.zip
文件大小	119.50 KB (122368 字节)

该样本是一个.net编译的PE文件，并且经过强混淆。

进行去混淆后效果如下所示：



其执行时，先解密初始化下载URL（https://158.247.208.174:443/mp4/ads.mp4）和AES解密所需要的KEY（LgUmeMnmUpRrCCRB）和IV（nStxRW4o6TNHcKBx），接着从服务器下载数据文件，并对数据文件进行AES解密再解压缩得到Shellcode,最后创建线程启动Shellcode。

Shellcode数据中内嵌了一份经过加密的Payload，Shellcode在执行过程中，会解密并内存加载最终的木马程序。

其最终恶意组件是一个Sliver程序，Sliver是一个开源的，Golang开发的跨平台C2框架（https://github.com/BishopFox/sliver/）。Sliver支持Windows，Linux，MACOS等多种系统，并支持多种通信协议。其功能包含文件操作，进程操作，提升权限，进程注入，横向移动、截屏、远程执行shell等多种功能。

除此以外，Sliver服务端在生成木马的时候，还可以对生成的木马函数名进行混淆。如下图，上方是并未添加混淆的样本，可以清楚地看到导入的模块信息。而下方是本次捕获的样本，可以看到函数的信息已经进行了混淆，经过分析，发现该程序C2为158.247.208[.]174。

总结

APT-C-01（毒云藤）组织从自披露后，从未停止相关攻击活动，并且极其擅长钓鱼攻击。在同时期，我们也发现该组织多次伪造知名邮箱进行网络钓鱼，从而获取用户信息，并

且伪装的钓鱼链接具有很强的迷惑性。因此在这里提醒相关企业和个人加强安全意识，切勿执行未知链接和未知样本，以免中招，从而导致敏感或重要信息的泄漏。

附录 IOC

MD5:

61c42751f6bb4efafec524be23055fba

3bd15b16a9595d20c0e185ab1fae738f

7f0dba2db8c3fdd717d83bb693b3ade9

88e306f4d6a33703316e794a9210f528

3a74ed8d1163d1dbc516410d1b8081fa

C2:

165.22.97[.]48

158.247.208[.]174

128.199.134[.]3
caac-cn[.]org
caac-cn[.]com

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，赢得业内外的广泛认可，为360保障国家网络安全提供有力支撑。