针对毒云藤（APT-C-01）组织近期的大规模钓鱼攻击活动披露

原创 高级威胁研究院 360威胁情报中心 3天前

收录于话题
#毒云藤

2个

概述

毒云藤（APT-C-01）组织是一个长期针对国内国防、政府、科技和教育领域的重要机构实施网络间谍攻击活动的APT团伙，其最早的攻击活动可以追溯到2007年。360高级威研究院10月11日独家发布的《毒云藤（APT-C-01）组织2020上半年针对我重要机构定向攻击活动揭秘》报告中披露了该组织上半年利用新冠肺炎等热点事件针对国内国防、政府等重要机构频繁的网络间谍攻击活动。

近期毒云藤组织的攻击活动并未减弱蛰伏，反而异常活跃。2020年6月，该组织技战术进行了调整，开始针对特定单一人物目标实施定向攻击。进一步8月初开始，我们发现该组织针对国内高等院校、科研机构等，进行了大规模邮箱系统钓鱼窃密攻击活动，涉及了大量的相关单位，相关攻击至今持续活跃。

利用社会工程学窃取邮箱密码

在近期集中的钓鱼攻击活动中，攻击者依然利用鱼叉邮件发送钓鱼链接的形式进行攻击，本次攻击与该组织以往相关钓鱼攻击技战术并无太大差异，只是攻击目标变化且范围增大，另外攻击频次大幅度增加。攻击者会根据目标角色精心设计钓鱼邮件，伪造目标角色身份相关的工作文档，诱使目标访问钓鱼网站获取附件，以盗取邮箱密码。

当被攻击目标访问到伪造的钓鱼网站后，会弹出伪造的登录框提示需要输入用户名和密码。

伪造QQ邮箱登陆

伪造网易邮箱登陆

只有目标用户填写了用户名和密码登陆钓鱼网站后，才能获取到相应的附件文件

仿冒高等院校电子邮件系统

在近期的攻击活动中，毒云藤组织针对一大批高等院校的邮件系统制作了钓鱼网站。以下是部分仿冒网页：

仿冒**大学电子邮件系统

仿冒**大学电子邮件系统

仿冒**大学电子邮件系统

定制目标角色相关的诱饵文档

毒云藤组织会根据目标角色定制不同内容的诱饵文档，这些文档都是正常的文件，通常与目标角色的工作内容紧密关联。

该组织近期攻击活动中使用的部分诱饵文件名：

文件名
******通知信
调研通知
国家******调查问卷
相关信息
青年******项目评议要点
关于调整******标准的通知
航天******需求
科技部******项目申报.docx

以下是部分诱饵文档的内容：

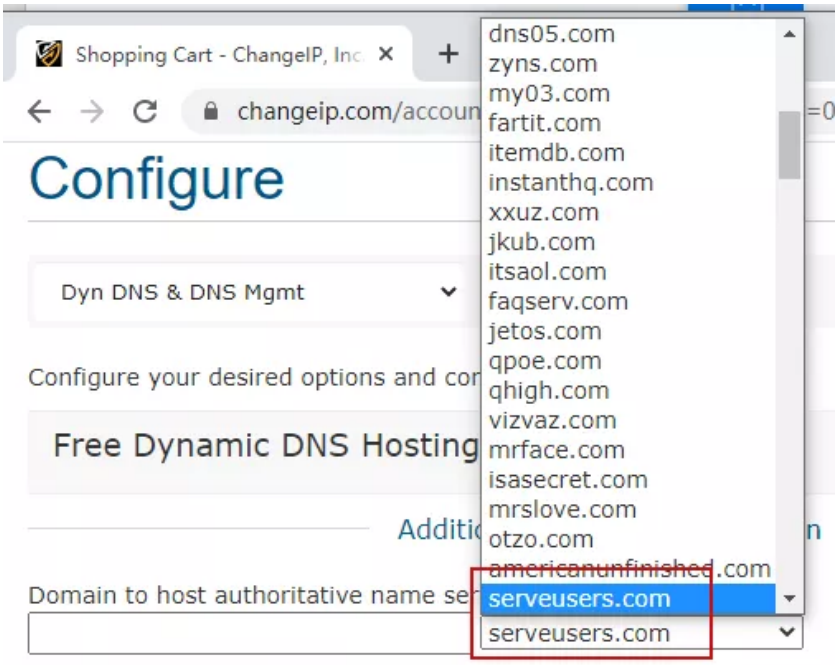
国家******调查问卷

******博览会

国防******

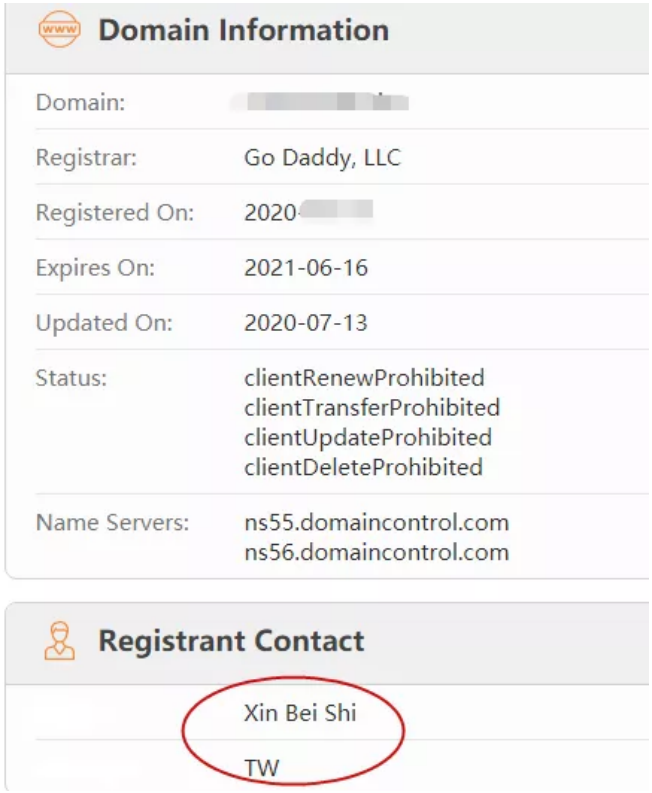
APT-C-01组织C2信息关联

- 部分C2与早期攻击活动动态域名供应商相同
  2018年9月20号，360披露了毒云藤(APT-C-01)组织， 在当时的披露的攻击活动中该组织使用的动态域名服务商changeIP占比最大，例如serveusers.com。而此次攻击活动中，攻击者依然热衷与使用动态域名，域名命名风格与早期已披露攻击活动中使用的相似，喜欢伪造成国内邮箱服务提供商的域名，例如count.163*.serveuser.com。



- 与其他攻击活动共用已暴露C2
  APT-C-01会使用一些已暴露的C2发起不同的攻击活动，我们注意到一些该组织已经暴露的C2（如141.164.*.*）的攻击活动为lnk诱饵安装木马后门程序，同时在该C2下也进行了钓鱼攻击。

- 部分钓鱼域名注册信息泄漏攻击人员地理位置
  由于APT-C-01组织的疏漏，我们发现部分钓鱼域名的whois信息泄漏了注册人员的真实地理位置。



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。

文章已于2020-10-13修改