沙猞猁组织—针对库尔德斯坦民主党（KDP）活动人士的攻击 | CTF导航

Archived: 2026-04-02 10:40:19 UTC

摘要

＊近日，奇安信病毒响应中心移动安全团队监测到两个伪装成库尔德斯坦民主党（KDP）相关网站移动端应用的MOrder RAT恶意样本。

＊受害者会被窃取走手机上的个人通讯录、短信和其他社交软件资料等敏感信息。
＊我们将该APT新组织命名为“沙猞猁”（Caracal Kitten），该组织是奇安信独立发现并全球率先披露的第16个APT组织，编号为APT-Q-58。
＊MOrder RAT默认向数据库指令表中插入“MCNT”和“MSMS”指令，用于窃取受害者通讯录和短信。
＊远控服务器使用FileZillaServer配置了FTP服务器转载，转移窃取到的受害者资料。

关键词： 库尔德斯坦民主党（KDP）、MOrder RAT、Ahmyth RAT、沙猞猁

概述

近日，奇安信病毒响应中心移动安全团队监测到两个伪装成库尔德斯坦民主党（KDP）相关网站移动端应用的样本。经过分析和挖掘，发现其为攻击库尔德斯坦民主党（KDP）活动人士的恶意软件，该恶意软件会窃取受害者的通讯录、短信和其他社交软件资料等敏感信息。

综合获取的情报，我们认为其攻击者较高概率为来自中东某政权背景的组织。该组织虽然与此前公开的Domestic Kitten、Ferocious Kitten和Rampant Kitten等组织有类似的攻击目标，但目前并未发现相关IOC资源和证据表明其归属于某一历史组织，且该组织具有更加明确的攻击目标，更清晰的攻击时间节点。我们根据该组织的攻击特点和组织特征，将其命名为“沙猞猁”，英文名“Caracal Kitten”，奇安信内部APT组织编号为APT-Q-58。沙猞猁是奇安信独立发现并全球率先披露的第16个APT组织。

公开情报显示，库尔德人是主要生活于西亚库尔德斯坦地区的游牧民族，总人口3000万，主要分布在土耳其、叙利亚、伊拉克、伊朗四国境内，在中东是人口仅次于阿拉伯、土耳其和波斯的第四大民族。库

尔德斯坦民主党（KDP）是库尔德人的一个民族政党，长期以来，与所属地区的政府和团体具有较复杂的关系。

第一章　　武器分析

本次攻击活动中，共捕获和挖掘出该组织2款武器，其一是伪装成库尔德斯坦民主党 (KDP) 中央网站和库尔德斯坦媒体移动端应用的MOrder RAT；其二是Ahmyth RAT的客户端样本。

01

MOrder RAT

本次捕获的样本，采用了集成软件开发平台进行开发，但是核心的远程控制代码为开发者开发，其远控命令都在功能缩写前加了“M”，客户端和服务器都将指令称为“order”，所以我们将此家族木马命名为“MOrder RAT”。

(一) 伪装情况

捕获的样本应用名称分别为“kurdistanukurd”和“KurdistanMedia”。除在应用显示图标上使用库尔德斯坦民主党 (KDP)标志外，应用内更是直接通过webview组件加载相应的官方网站链接，分别为“https://kurdistanukurd.com/”和“https://kurdistanmedia.com/”，可以正常使用，具有很强的迷惑性。相应的应用运行后伪装的交互界面如下：

(二) 远控功能

恶意样本启动后，进行初始化服务，C2服务器地址为“http://65.109.157.77”，初始化源码示例如下：

远控功能目前主要窃取受害者的通讯录、短信和其他社交软件资料等。移动端编写的指令和功能如下表：

指令	功能
MINFO	上传设备与授权信息

MCNT	上传通讯录
MSMS	上传短信
MLS	上传SD卡文件树
MSNDM	向指定电话发送短信
MMSG	Toast提示信息
MDWN	上传指定文件
MBRW	开启指定界面

受害者在安装运行样本后，会自动进行注册，与此同时，根据其服务器源码显示，会默认向数据库指令表中插入“MCNT”和“MSMS”指令，用于窃取受害者通讯录和短信。注册源码如下：

其他的远控指令更像是针对特定受害者的精准定制化指令，通过另一个服务器接口动态插入到数据库指令表中，受害者及对应指令示例如下：

02

Ahmyth RAT

(一) Ahmyth 介绍

Ahmyth 是一个开源的Android远程控制项目，分为服务器端和客户端，该项目常被用来制作Android端的RAT样本。其包含录音录屏拍照、获取设备文件、获取定位、获取联系人短信和通话记录及发送短信等功能。服务端控制界面示例如下：

(二) 样本分析

在此次攻击事件中，我们发现该组织制作了相关的Ahmyth RAT样本作为其攻击武器，然而并未发现其受害者，怀疑此武器还在制作测试阶段，暂未进行载荷投递和攻击使用。

在其制作的Ahmyth RAT样本中，使用的远控服务器与上面介绍的伪装应用使用的远控服务器相同，都为“65.109.157.77”。样本源码截图如下：

第二章　　攻击时间线

由于攻击者的服务器配置不当，该服务器泄露了受害者数据。通过对泄露出来的服务器上的受害者数据进行分析，我们发现该组织的攻击活动具有很明显的时间节点，大体可以分为两段。

首次攻击时间为2021年7月至11月，最新一次攻击始于2023年5月延续至今。其中首次攻击时泄露的受害者部分数据如下：

第三章　　受害者分析

此次攻击目标比较明确，诱饵是伪装成库尔德斯坦民主党（KDP）相关网站的移动样本。由于主控服务器使用FileZillaServer配置了FTP服务器转载，因此我们并未获取到大量的受害者历史资料，用于判断更多受害者具体身份。

根据以下受害者资料，结合诱饵特征我们认为此次攻击活动是针对库尔德斯坦民主党（KDP）活动人士的攻击。

01

受害者数据库数据

在其泄露的受害者用户表中，可以看到众多的库尔德语受害者名字。

02

受害者通讯录

在受害者通讯录文件中，姓名几乎全部采用库尔德语语言，电话号码大多数为伊朗号码，还含有少量的伊拉克号码，值得说明的是库尔德斯坦民主党（KDP）相关网站上联系电话也为伊拉克号码。受害者通讯录示例如下：

在通讯录中，我们追踪了部分联系人身份，示例是一个与库尔德人相关的线上哀悼的社交账号帖子，其中发现了通讯录中的联系人电话，姓名也大致相符，示例如下：

第四章　　组织归因

分析追踪中，我们发现该组织具有很强的隐匿能力和谨慎的风格。其通过其他代理服务器和移动网络远程操控主要服务器，并及时的将受害者数据进行转载和清理。

在深入的情报分析后，我们基于以下几点证据，怀疑其攻击者为具有中东某政权背景的组织，并结合该组织攻击特点和组织特征，将其命名为“沙猞猁”，沙猞猁是一种领域性非常强的猫科动物，外表和猞猁很像，善于隐藏，可以长时间不喝水而持续存活，曾在某些中东国家被驯化当做猎猫。

01

时区设置

在对泄露的源码和受害者数据进行分析时，发现未在样本中显式使用的时间时区设置为中东某地区，相关时区设置源码截图如下：

02

指令下发服务器追踪

在泄露的源码中，我们发现除自动插入的“MCNT”和“MSMS”指令外 ，其他指令都通过另一接口远程插入到指令表，而此接口是没有在已捕获的攻击样本中使用过的。

通过我们的技术追踪，我们发现访问此接口的ip地址中大部分来自中东某国的移动服务和通信公司，此外还有用于FTP服务器转载的服务器ip“193.36.85.60”和其他代理服务器。访问此接口的ip地址及溯源信息列表如下：

IP	**Organization**
5.121.14.188	IRANCELL
5.121.146.166	IRANCELL
5.121.152.16	IRANCELL
5.121.173.251	IRANCELL
5.121.206.148	IRANCELL
5.121.33.182	IRANCELL
5.121.37.94	IRANCELL
5.121.47.140	IRANCELL
5.121.48.51	IRANCELL
5.121.70.103	IRANCELL
5.122.1.36	IRANCELL
5.122.128.28	IRANCELL

5.122.133.119	IRANCELL
5.122.169.163	IRANCELL
5.122.210.220	IRANCELL
5.122.212.228	IRANCELL
5.122.252.153	IRANCELL
5.122.78.188	IRANCELL
5.122.89.51	IRANCELL
5.122.96.113	IRANCELL
144.76.200.143	Hetzner
193.36.85.60	ORG-TMYS3-RIPE
23.95.44.219	Vortexlayer Online Solutions LLP

03

开发者指纹

开发者在开发软件的过程中，容易因疏忽而留下一些开发者指纹信息，如开发时的调试log信息。在本次的攻击样本中，虽然大部分为开发框架源码，核心源码中log信息都采用了英语和数字标识，但还是有一处关键位置的log信息泄露，此处log采用硬编码的波斯语输出调试信息。源码截图如下：

04

情报关联

在我们进行情报搜集时，发现库尔德斯坦民主党（KDP）网站曾发布过一篇文章，在文章中声称“某政权将名为kurdistanukurd.apk的文件通过社交网络等方式向库尔德活动人士投递，以此来获取手机和个人信息，此类文件经常有活动人士和政党的名义和内容发布，特别是与明珠当关系密切的网站，而大多数防病毒软件无法处理这种病毒，也无法破解它。”。

经过我们的分析与确认，文中提到的恶意文件与此次我们发现的样本为同一家族样本。库尔德斯坦民主党（KDP）网站文章详情如下：

第五章　　总结

沙猞猁组织（APT-Q-58）使用低成本、轻量便捷的武器，采用移动网络和远程代理服务器转载控制，都给对其活动的捕获、追踪和关联增加了难度。针对特定人群如何避免遭受移动端上的攻击，奇安信病毒响应中心移动安全团队提供以下防护建议：

01

及时更新系统和应用，在正规的应用商店下载应用。国内的用户可以在手机自带的应用商店下载，国外用户可以在Google Play下载。不要安装不可信来源的应用、不要随便点击不明URL或者扫描安全性未知的二维码。

02

移动设备及时在可信网络环境下进行安全更新，不要轻易使用不可信的网络环境。

03

不轻易开启Root权限；对请求应用安装权限、激活设备管理器等权限的应用要特别谨慎，一般来说普通应用不会请求这些权限，特别是设备管理器，正常的应用基本没有这个需求。

04

确保安装有手机安全软件，进行实时保护个人财产安全；如安装奇安信移动安全产品。

目前，基于奇安信自研的猫头鹰引擎、QADE引擎和威胁情报数据的全线产品，包括奇安信威胁情报平台（TIP）、奇安信天狗漏洞攻击防护系统、天擎、天机、天守、天眼高级威胁检测系统、奇安信NGSOC（态势感知与安全运营平台）、奇安信监管类态势感知等，都已经支持对此类攻击的精确检测。

IOCs

MD5	C2
9a4375a519fc11dce701ae830f833407	65.109.157.77
426453b2c7beaaf275270daff8df4679	65.109.157.77
1453e01437e5ccdde646f50647e9535b	65.109.157.77:42474

附录1 奇安信病毒响应中心

奇安信病毒响应中心是北京奇安信科技有限公司（奇安信集团）旗下的病毒鉴定及响应专业团队，背靠奇安信核心云平台，拥有每日千万级样本检测及处置能力、每日亿级安全数据关联分析能力。结合多年反病毒核心安全技术、运营经验，基于集团自主研发的QOWL和QDE（人工智能）引擎，形成跨平台木马病毒、漏洞的查杀与修复能力，并且具有强大的大数据分析以及实现全平台安全和防护预警能力。

奇安信病毒响应中心负责支撑奇安信全线安全产品的病毒检测，积极响应客户侧的安全反馈问题，可第一时间为客户排除疑难杂症。中心曾多次处置重大病毒事件、参与重大活动安全保障工作，受到客户的高度认可，提升了奇安信在业内的品牌影响力。

附录2 奇安信病毒响应中心移动安全团队

奇安信病毒响应中心移动安全团队一直致力移动安全领域及Android安全生态的研究。目前，奇安信的移动安全产品除了可以查杀常见的移动端病毒木马，也可以精准查杀时下流行的刷量、诈骗、博彩、违规、色情等黑产类软件。通过其内部分析系统可以有效支持对溯源分析等追踪。

团队结合自研QADE引擎和高价值移动端攻击发现流程已捕获到多起移动攻击事件，并发布了多篇移动黑产报告，对外披露了多个APT组织活动。近三年来已首发披露五个全新APT组织（诺崇狮组织SilencerLion、利刃鹰组织BladeHawk、艾叶豹组织SnowLeopard、金刚象组织VajraEleph和此次的沙猞猁组织Caracal Kitten）。

未来我们还会持续走在全球移动安全研究的前沿，第一时间追踪分析最新的移动安全事件、对国内移动相关的黑灰产攻击进行深入挖掘和跟踪，为维护移动端上的网络安全砥砺前行。
