

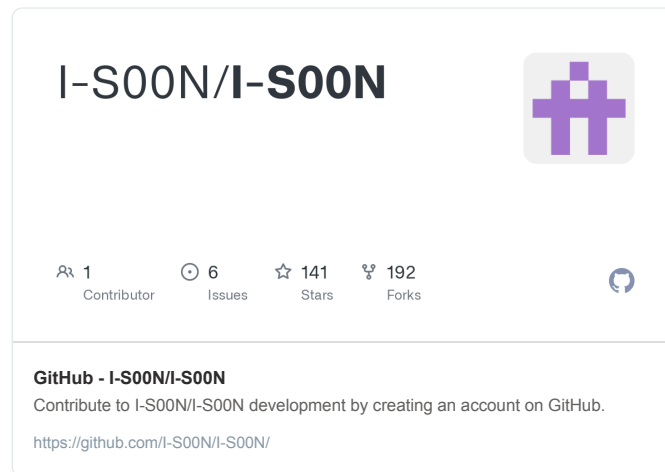


安坂星海 Azaka 🐼 VTuber @AzakaSekai\_

Feb 18, 2024 · 39 tweets · [AzakaSekai\\_/status/1759326049262019025](#)

#threatintel

someone just leaked a bunch of internal Chinese government documents on GitHub



From the looks of it, it looks like a bunch of spyware developed by the company 安洵信息

Some of these software features includes obtaining the user's Twitter email and phone number, realtime monitoring, publishing tweets on their behalf, reading DMs.

### 1.2.2 产品功能

- **Twitter 注册信息查询：**平台支持根据 Twitter 账号查询注册时使用的手机号码和邮箱。
- **Twitter 账号反制：**平台可根据用户指定链接（真实存在或是自定义链接）生成取证链接，发送给目标并诱导其点击并进行相关操作，即可实现目标 Twitter 私信获取，推文发送/删除/转发/评论/点赞。
- **Twitter 账号监控：**平台支持对 Twitter 账号进行实时监控，第一时间更新目标 Twitter 账号的动态信息。

### 1.2.3 行业优势

- 查询速度快——根据提交的目标信息，3-5 分钟返回查询结果。
- 数据更新快——系统目前每天跑的原始数据量不少于一亿条数据，并支持每天实时更新可用数据。
- 无感获取目标信息——通过取证链接，后台系统可快速登陆目标人 Twitter 账户进行操作，无需目标人物的账号密码，降低目标人员警惕防线。
- 功能全面——通过对目标人员 Twitter 账号权限的获取，后台可直接对 Twitter 账号进行操作，全面控制目标人 Twitter 账号。

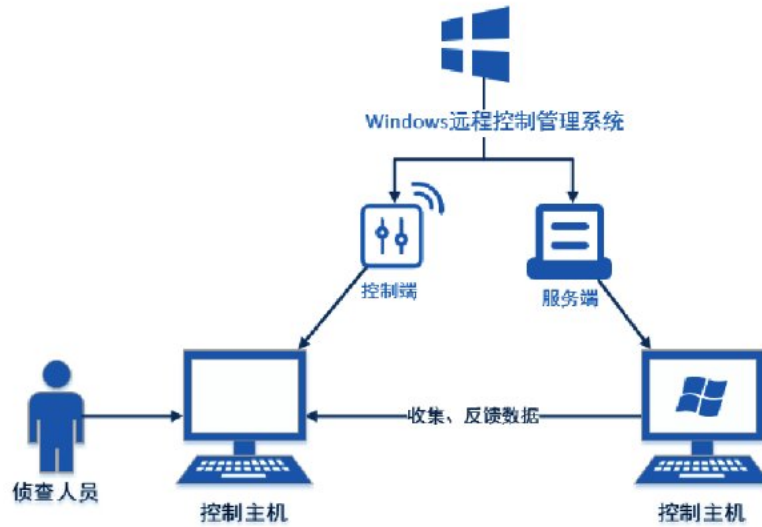
Custom RAT built for Windows x64/x86 with features such as process/service/registry management, remote shell, keylogging, file access logging, obtaining system info, disconnect, uninstallation.

## 1.3 Windows 远程控制管理系统

### 1.3.1 产品简介

Windows 远程控制管理系统基于当前主流网络架构和 Windows 系统环境自主研发，实现对 Windows 系统的远程操作、监控和取证。

系统主要由生成器和控制器组成，通过将生成器生成的程序植入到目标主机并运行，侦查人员在控制器端则可以看到目标主机的上线信息，并根据侦查人员的指令，将目标主机的数据返回给侦查人员。



(Windows 远程控制管理系统运行形态图)

### 1.3.2 适用环境

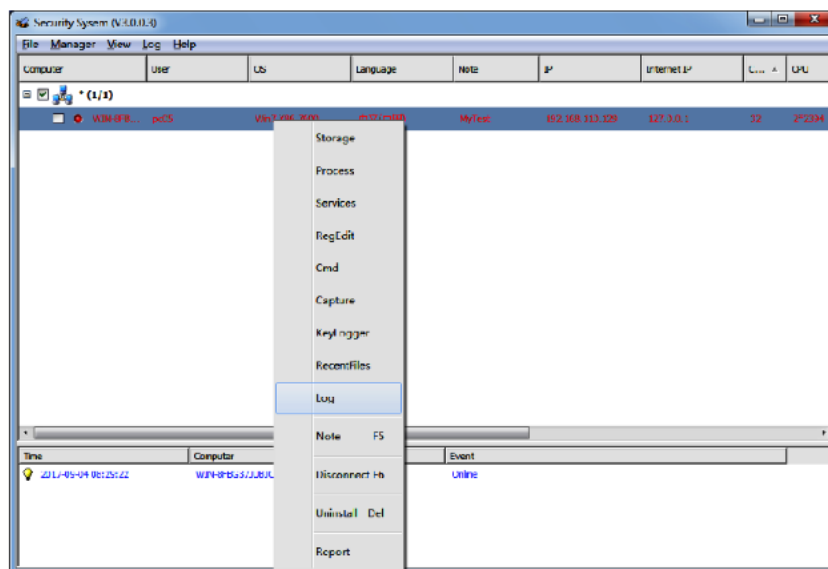
操作系统位数	操作系统版本
x86	Windows XP/Vista/7/8/8.1/10 Windows Server 2003/2008/2012/2016
x64	Windows Vista/7/8/8.1/10 Windows Server 2008/2012/2016

- **进程管理：**支持对目标操作系统上运行的应用进程、后台进程、Windows 进程等进行实时监控和控制。包括查看、刷新、结束等操作。
- **服务管理：**支持对目标操作系统的各项服务状态实时远程管理。包括运行、暂停、停止、删除等操作。
- **注册表管理：**支持对操作系统注册表的远程管理。包括查看相关程序的注册表信息、对注册表信息进行修改、删除等操作。
- **CMD 控制台：**支持对目标操作系统进行 CMD 命令操作。
- **屏幕截图：**支持对目标操作系统的电脑进行屏幕截图操作。
- **键盘记录：**支持对目标在操作键盘时按下的每个按键进行记录。
- **文档访问记录：**支持对目标最近访问的文件进行记录。
- **上线日志记录：**支持对目标主机的上线、下线时间等日志进行记录。
- **远程修改配置：**被控端上线后，系统支持远程修改目标机上线地址和注入进程信息。
- **内网级联上线：**系统支持 TCP、UDP 和网络自动互联协议三种方式上线，支持同一局域网内不能上互联网的 PC 通过能上网的 PC 上线回传。
- **导出上线主机信息：**支持导出上线的主机的基本信息，包括：上线主机名、内网 IP 地址、外网 IP 地址、主机内存、硬盘、CPU、网速等系统运行和使用的状态信息。
- **断开连接：**系统具有主动断开连接功能，在主动断开连接后，被控端支持对上线域名 DNS 解析或者上线 IP 地址的实时刷新。
- **卸载服务端：**在控制监管结束后，被控端操作系统支持远程卸载服务。

The documentation contains a screenshot of the controller, titled Security System (V3.0.0.3)

- 免杀性强——系统采用业内独有的突破杀软主动防御技术，免杀能力强，能够躲避市面上 95% 杀毒软件的查杀，如国内 360、金山杀毒、腾讯电脑管家；国外卡巴斯基、赛门铁克、麦咖啡等主流杀毒软件。并且基于内存多态变形制作和文件多态制作双重技术，可有效躲避内存动态扫描和文件静态扫描防护机制。
- 隐蔽性强——支持被控端程序安装后自启动、自删除，并且支持相关程序安装成功后，自动删除安装文件。
- 应用性广——支持主流 x86/x64 Windows 操作系统(包括最新的 Win10)。
- 易用性佳——整个系统的界面简洁、操作简单、方便用户快速上手。

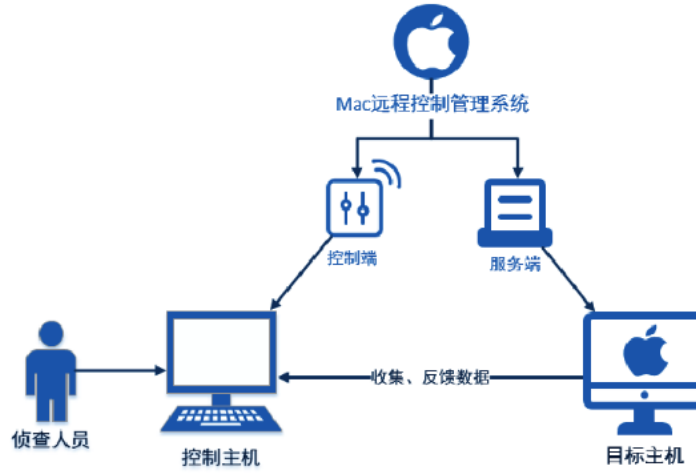
### 1.3.5 产品图片



(Windows 远程控制管理系统界面图)

A Mac version also exists, with features such as remote shell, file management, screenshot and keylogging.

系统由控制端和服务端两个部分组成，控制端采用 C/S 架构，用户通过控制端发送对目标计算机的控制指令，服务端接收到指令后执行用户对目标计算机的控制操作。



(Mac 远程控制管理系统运行形态图)

#### 1.4.2 适用环境

程序	支持的操作系统
控制端	全面兼容 Windows NT、Windows2000、WindowsXP、Windows 2003 VISTA、Windows7 等多种操作系统
服务端	兼容苹果操作系统全版本

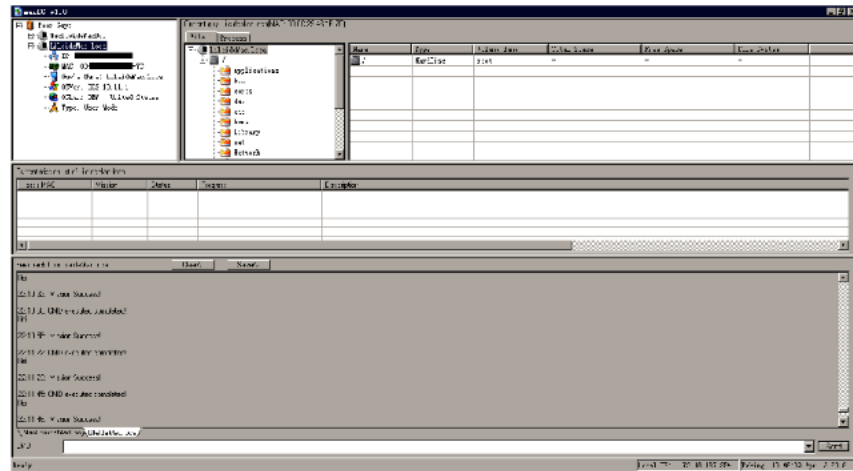
### 1.4.3 产品功能

- **信息管理：**控制台界面支持显示出目标苹果机上的计算机名称、用户名、操作系统内核及当前发布的版本信息等内容。
- **文件管理：**支持对目标计算机的文件执行创建、上传、下载（支持断点续传）、删除、重命名等操作。
- **Shell 命令：**支持对目标端的电脑进行 Shell 命令操作。
- **屏幕截图：**支持对目标端的电脑进行屏幕截图操作。
- **键盘记录：**支持对目标在操作键盘时按下的每个按键进行记录。

### 1.4.4 行业优势

- 隐蔽性强——服务端植入目标电脑后无启动项，保证目标计算机全程无感。
- 兼容性强——能兼容苹果操作系统全版本。
- 稳定性高——系统支持 24 小时不间断运行，并具备自我恢复的容错机制。
- 传输取证速度快——服务端与客户端网络在 10M 情况下，文件下载速度  $\geq 200\text{Kb/S}$ ，文件上传速度  $\geq 100\text{Kb/S}$ ，屏幕截取速度  $\geq 5$  帧/分。
- 连线指标高——最大连接端  $\geq 2000$  个，并发连接 100 个服务端情况下，系统依然可正常工作。

### 1.4.5 产品图片



(Mac 远程控制管理系统界面图)

An iOS version also... exists somehow, and they claim that this supports all iOS versions. Includes features such as gathering hardware information, GPS data, contacts, media files, and real-time audio record. No jailbreak required.

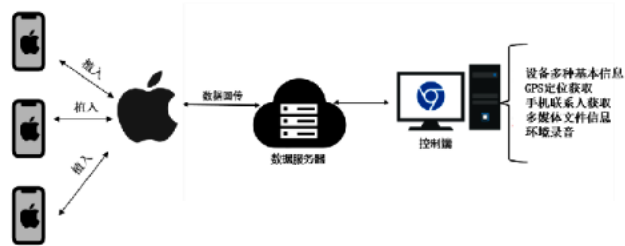


## 1.5 iOS 远程控制管理系统

### 1.5.1 产品简介

iOS 远程控制管理系统是一款专门针对运行 iOS 系统的 iPhone 设备进行免越狱安装的远程信息获取系统，可实现对 iOS 系统的设备进行远程取证和监控。

专业的数字情报解决方案提供商



(iOS 远程控制管理系统运行形态图)

### 1.5.2 适用环境

机型	系统
iPhone 全型号	iOS 全版本

(iOS 远程控制管理系统运行形态图)

### 1.5.2 适用环境

机型	系统
iPhone 全型号	iOS 全版本

### 1.5.3 产品功能

- **手机基本信息获取：**获取目标 iOS 系统设备的唯一标识符、IP 地址、MAC 地址、设备版本信息。
- **GPS 定位获取：**定时获取目标 iOS 系统设备的 GPS 定位信息。
- **手机联系人获取：**获取目标 iOS 系统设备的通讯录联系人。
- **多媒体文件：**获取目标 iOS 系统设备的多媒体文件信息。
- **录音：**支持定时获取目标 iOS 系统设备的环境录音。

### 1.5.4 行业优势

- **免越狱——**创新的方式将控制系统植入到设备中运行，无需越狱即可获取目标数据信息。
- **兼容性强——**兼容 iOS 系统全系列的智能硬件设备。
- **行业领先——**率先在全国领先推出针对 iOS 系统的远程控制管理系统，并且能够结合相关执法部门业务场景应用于实战，实现对目标 iOS 系统设备数据信息的获取。

### 1.5.5 产品图片



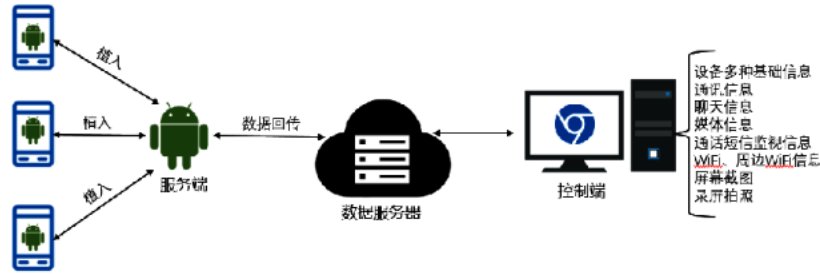
(iOS 远程控制管理系统界面图)

Android version also exists, supporting Android 6.0 and above. Features include obtaining system information, GPS, contacts, SMS, call logs, browser history, app list, real-time audio recording, process list, camera, WiFi list, screenshot, keylogging, and system info.

## 1.6 Android 远程控制管理系统

### 1.6.1 产品简介

Android 远程控制管理系统基于远程控制技术实现电子数据远程提取。系统由控制端和服务端两部分组成，控制端采用 B/S 架构，服务端可安装在多种主流 Android 设备上，安装完成后自动上线连接控制端，服务器支持不低于 200 个远控系统承载。



(Android 远程控制管理系统运行形态图)

### 1.6.2 适用环境

类型	项目
----	----

Few interesting tidbits for the Android one

- Ability to dump messages from QQ, WeChat, and MoMo - all popular Chinese IM apps (requires root)
- Ability to keylog specifically QQ, WeChat, Momo \*AND\* Telegram.
- Ability to elevate as system app for persistence (requires root)

➤ **多种聊天信息获取：**支持获取手机上包括微信、QQ、陌陌聊天软件的联系人和聊天记录。（需要 root）

➤ **键盘监听：**支持截取手机在使用 QQ、微信、陌陌、Telegram 应用时输入的文本信息。（需开启内存清理服务且 Android4.2 及以后版本有效）

● **驻留性强——**支持提升为系统 APP(需 ROOT 权限)，即使 Android 设备重装系统，程序依然存在。

## Controller for the Android RAT

专业的数字情报解决方案提供商

### 1.6.5 产品图片



The screenshot displays a web-based interface for managing an Android device. At the top, there is a navigation bar with icons for various functions: 基本信息 (Basic Info), 定位 (Location), 联系人 (Contacts), 微信 (WeChat), 文件管理 (File Management), 网络痕迹 (Network Traces), 软件列表 (App List), 录音文件 (Audio Files), 摄像头 (Camera), 无线网络 (Wireless Network), 键盘监听 (Keystroke Monitoring), and 蓝牙 (Bluetooth). Below the navigation bar, the device status is shown as '小米5 (在线: Wifi, 电量: 64%, 屏幕: 亮屏)'. A row of status icons includes 获取权限 (Get Permissions), 联网 (Online), 更新客户端 (Update Client), 网络客户端 (Network Client), and 服务责任书 (Service Responsibility Statement). The main content area is divided into two sections. On the left is a table of device details, and on the right is a control panel for the mobile network.

MAC地址	b0:e2:00:00:00:00
电话	
IMEI号	460008 中国移动
IMEI号	86132
客户版本号+验证码	非ROOT版 2.0.5 (1205-2.0.5test)
接入系统时间	2016-12-05 19:50:13
系统版本	6.0.1
手机制造商	gemin
硬件制造商	
系统定制商	Xiaomi
手机型号	MI 5
辅助功能状态	开
设备管理状态	关

右侧控制面板包含以下按钮：  
- 联系人: 432  
- 短信: 2042  
- 通话记录: 3635

底部标注: (Android 远程控制管理系统界面图)

Linux version also exists that specifically supports CentOS 5/6/7 & Ubuntu 12/14. Oddly old versions of these distros. Features include remote shell, file management, Socks5 proxy via SocksCap64, port reuse. Controller appears to be named "TracedStone"

### 1.7.2 适用环境

程序	操作系统位数	操作系统版本
被控端 (客户端)	x86/x64	Centos 5
		Centos 6
		Centos 7
	x64	Ubuntu 12
		Ubuntu 14
控制端	Windows XP/7/8, Windows Server 2003/2008, 支持多语言环境	

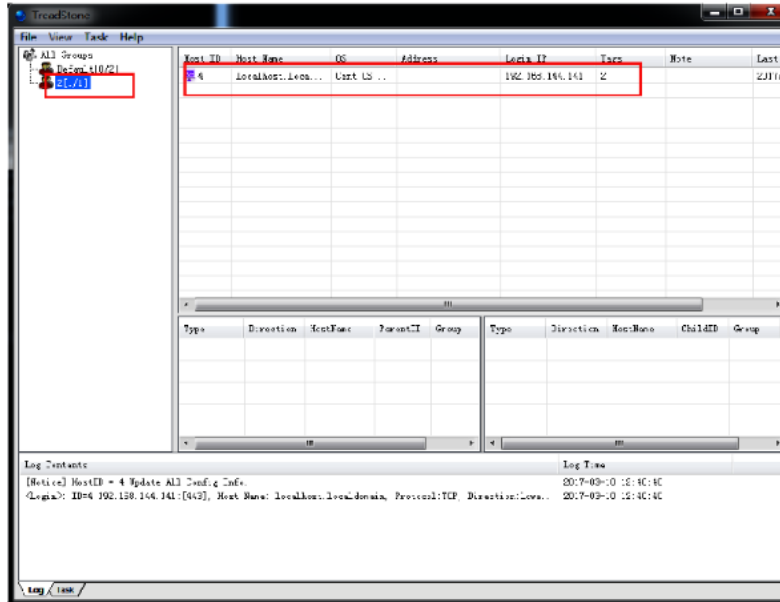
### 1.7.3 产品功能

- **Shell 命令:** 在控制端 Shell 界面上可以对客户端执行 Shell 命令操作。
- **文件管理:** 在远程管理界面上, 可以对目标计算机的文件和目录进行查看、删除、上传、下载等操作。
- **Socks5 代理:** 系统支持使用 SocksCap64 工具进行 socks5 代理, 同时支持查看被控端 Socks5 代理信息。
- **TCP 端口复用:** 系统支持在已开放的端口上进行通讯, 对输入的信息只进行字符匹配, 不对网络数据进行任何拦截、复制类操作, 实现端口复用的功能。

### 1.7.4 行业优势

- 兼容性高——系统支持级联技术, 并且支持 ICMP\TCP\UDP 三种协议进行传输。
- 稳定性高——系统支持 7\*24 小时稳定运行, 并具备自我恢复的容错机制。
- 隐蔽性强——支持复用 TCP 端口, 为实现远程控制系统预留后门。
- 易用性佳——可根据目标网络环境的特殊性, 选择不同的上线模式 (直连模式或反弹模式) 设置客户端上线。
- 免杀性强——针对国内外杀毒类软件定期测试, 保障工具正常使用需求, 可做到国内外主流杀毒软件免杀, 如 AVG\Clam\Comodo\卡巴斯基等主流 Linux 系统杀毒软件。

### 1.7.5 产品图片



(Linux 远程控制系统界面图)

This is the weirdest of them all - a WiFi-capable device that can inject into the targeted... Android devices via WiFi? The device is said to be portable, plug and play, supports 3G and 4G. After a successful injection, it can get device info, GPS, SMS, contacts, call log, files

## 1.8 WiFi 无感植入设备

### 1.8.1 产品简介

WiFi 无感植入设备是一款便携式的硬件设备，针对连接在设备 WiFi 上的安卓终端，实现特定软件无感植入，植入安装后可自动获取终端设备中的关键数据，并可视化展示。



(WiFi 无感植入设备运行形态图)



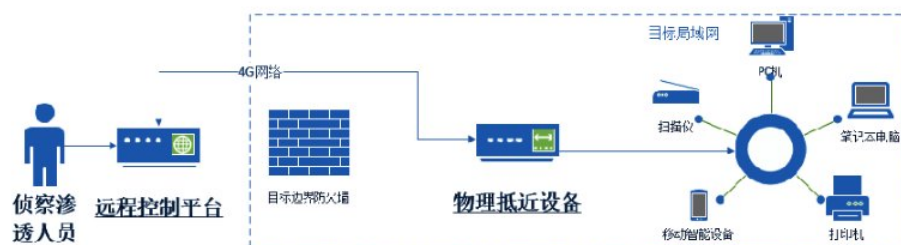
## 2.1 WiFi 抵近攻击系统

### 2.1.1 产品简介

WiFi 抵近攻击系统基于近场抵近攻击的渗透思想研发，实现远程操纵抵近设备渗透目标内网的目的，提高渗透的隐蔽性、便捷性和精准性。

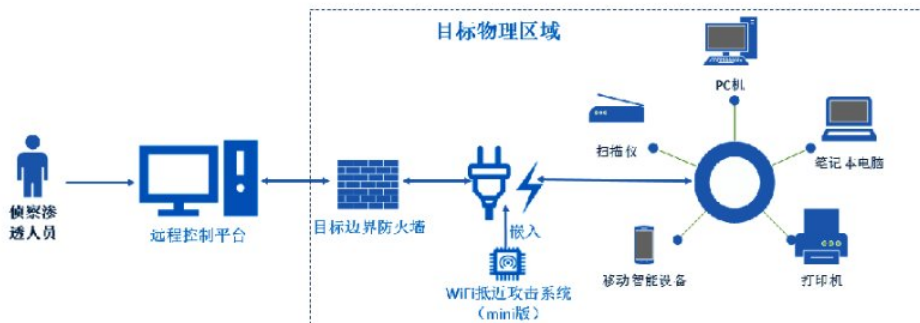
整个系统分为两个版本，包括：WiFi 抵近攻击系统（基础版）和 WiFi 抵近攻击系统（mini 版）。

基础版系统采用远近端相结合的架构设计，远程控制平台部署在公网服务器，负责下达攻击指令，抵近设备在目标物理区域执行命令开展渗透工作。



（WiFi 抵近攻击系统（基础版）运行形态图）

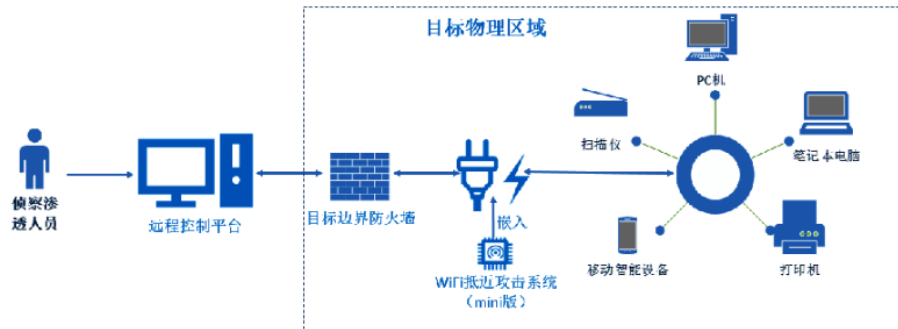
mini 版系统支持伪装成电源插排、电源适配器等形态，将设备放置在目标物理区域后，连接目标区域内 WiFi，建立 Socks 代理隧道，实现对目标网络的抵近渗透。



The Mini version is said to be able to disguise as a power strip, power adapter etc. and can be set up to connect to target WiFi and establish a SOCKS tunnel with the internal network.



mini 版系统支持伪装成电源插排、电源适配器等形态，将设备放置在目标物理区域后，连接目标区域内 WiFi，建立 Socks 代理隧道，实现对目标网络的抵近渗透。



(WiFi 抵近攻击系统 (mini 版) 运行形态图)

The standard version comes with 4G ability, 8GB eMMC, dual core 1.2GHz ARM processor, 10000 mAh battery, whilst the mini version runs on MIPS with 128MB of DDR2(?) and does not contain a battery.

### 2.1.3 产品参数

项目	WiFi 抵近攻击系统（基础版）	WiFi 抵近攻击系统（mini 版）
架构	ARM	MIPS
CPU	主频 1.2G，双核心	/
存储	8GB eMMC 高速闪存	DDR2 128MB
网络	支持全网通 4G	无线网卡 802.11/b/g/n 三种模式
内置电池	10000mA 充电锂电池	无
MCU 主频	/	580MHz
Flash	/	32MB
WiFi 模块	默认模式	支持 AP/STA 及 AP/STA 混合模式
设备详情	141mm x 73mm x 22mm	41mm x 23mm x 3.5mm

### 2.1.4 行业优势

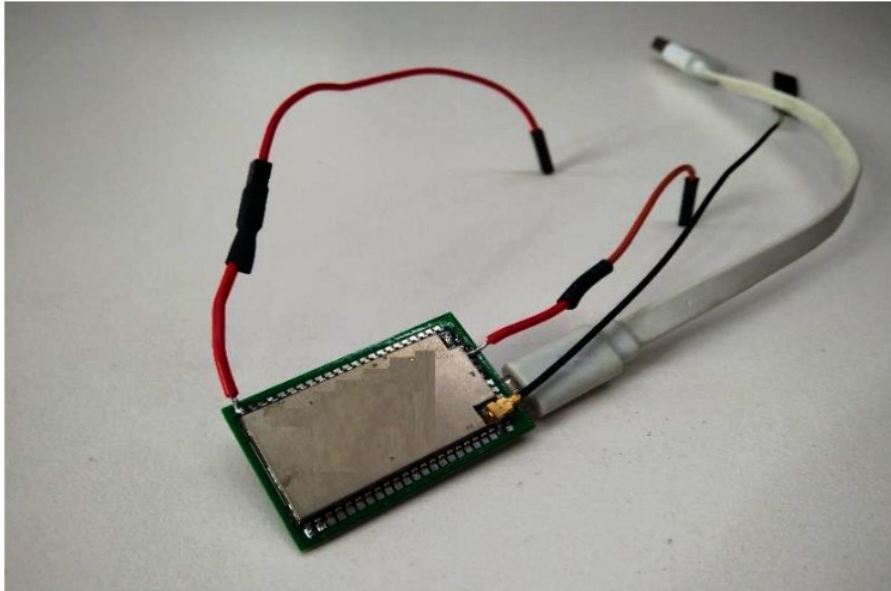
- 伪装性强——根据应用场景不同可选择不同版本，伪装成小米充电宝形态或者超小型电路板模块设计，便于携带且不易察觉，可通过安检、盘查等安保手段。
- 易用性高——只需携带设备到达指定区域后打开电源无需其他操作，远端即可控制设备开展渗透工作。
- 渗透效率高——产品硬件物理抵近与后台网络远程控制结合，为渗透工作建立新的内网渗透通道。
- 高续航能力——基础版内置大容量充电锂电池，满负荷续航 8 小时，常规运行续航 20 小时，并支持工作运行和充电过程同时进行。
- 操作方便——系统设置界面简单，均采用图形化界面，只需点击相关按钮即可完成操作。

The standard version is disguised as a Xiaomi battery, whilst the mini version is just a plain PCB that can be inside anything.

### 2.1.5 产品图片



(WiFi 抵近攻击系统 (基础版) 产品实物图)



(WiFi 抵近攻击系统 (mini 版) 产品实物图)

The Standard edition can be used to crack WiFi passwords, LAN port sniffing, SOCKS tunnel, port projection, remote shell, file management, and remote detonation (self-destruct).

### WiFi 抵近攻击系统（基础版）

- **WiFi 密码破解：**系统支持对目标区域范围的 WiFi（包括隐藏 WiFi 以及 5G\_WiFi）进行扫描破解，常见的 WEP、WPA、WPA2 和 WPS 协议均可进行破解。破解方式：本地云查询、云破解。
- **内网嗅探：**当抵近设备在目标内网域环境下时，设备主动嗅探目标内网域用户哈希并且自动抓取。
- **Socks 代理：**系统支持设置 Socks 代理功能，将内网信息映射到公网上进行相关渗透操作。
- **路由破解：**系统支持对目标内网存在的路由设备登录密码进行自动破解，以实现目标内网路由设备的主动登录和管理控制。
- **端口映射：**抵近设备通过 WiFi 接入目标内网后，可将内网中目标主机端口映射到互联网上，实现从外网访问目标内网的目的。
- **交互终端：**系统支持执行 Shell 命令，对抵近设备进行文件操作。
- **文件管理：**系统支持对抵近设备中的文件进行可视化上传、下载管理。
- **远程销毁：**抵近设备存在安全威胁时，支持远程发送自销毁指令，彻底清空设备内的所有系统数据。

### WiFi 抵近攻击系统（mini 版）

- **网络连接：**设备放置在目标网络环境后，通过其自带 WiFi 信号进行连接设置，最终实现连接到目标网络。
- **Socks 代理：**设备连上目标网络后，通过 PC 登陆远程控制管理系统，打开 Socks 代理即可进行相关渗透操作。

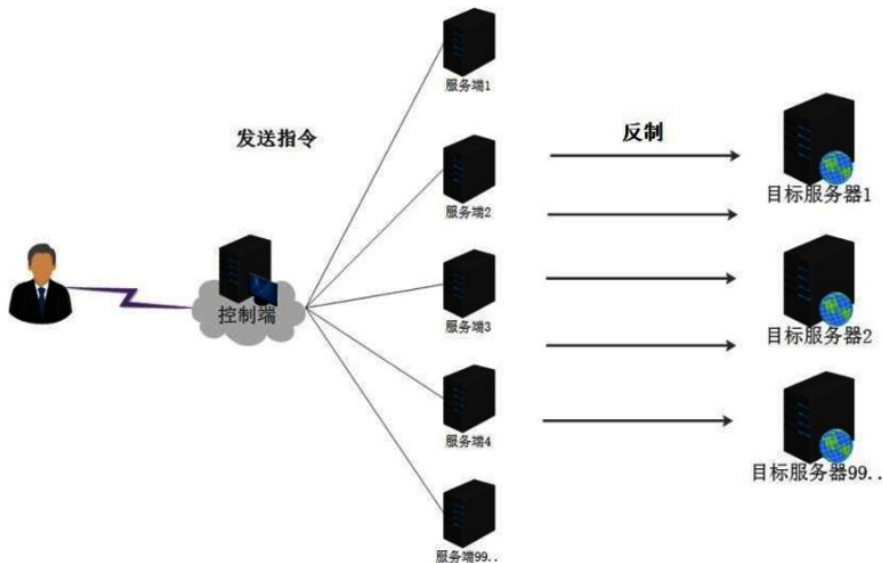
Correction: technically not Chinese government data, but a spyware vendor contractor's internal data.

Next chapter, they also have a DDoS system. The botnet client is 29kb sized and can be deployed on to Windows, Linux, or generic IoT devices with the total throughput of 10~100Gbps (or GBps? not specified).

## 2.2 网络流量反制系统

### 2.2.1 产品简介

网络流量反制系统结合相关部门实战应用场景，采用主动式扫描获取技术，获取全球分布式压力测试流量，实现对目标服务器、网站、企业网络等系统流量的全面反制。整套系统由反制流量获取模块和反制流量控制模块组成。



(网络流量反制系统运行形态图)

系统为 C/S 和 B/S 架构并存，充分吸收两种架构的特点。反制流量获取模块采用主动式扫描获取技术，获取全球存活网络流量并且进行综合性自动化海量漏洞探测，实现为反制流量控制模块提供网络流量数据。

反制流量控制模块用于控制所有节点并将接收到的反制指令进行统一下发。并提供专用匿名链路进行安全、高效的数据通信，使用过程中，系统支持多种对外接口，方便用户进行二次开发。

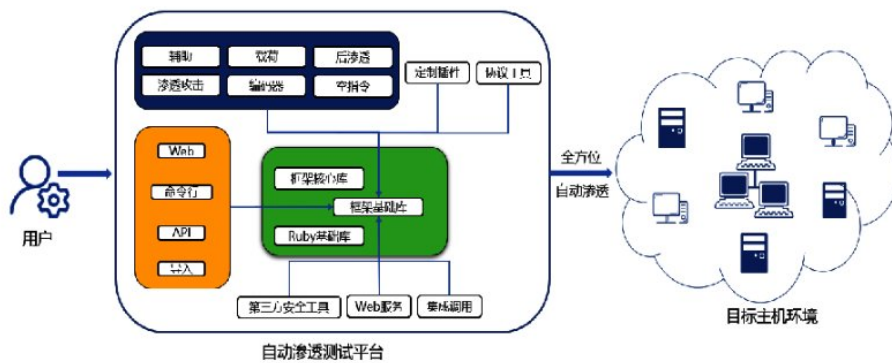
### 2.2.3 产品参数

项目	参数
扫描方式	异步传输
扫描线程	最大 1000
最大并发任务	20 个
漏洞类型	远程代码执行、弱口令、数据库、Web 等
上线数量	30000—60000
流量输出规模	10G—100G
客户端体积	29Kb
通讯模式	TCP/HTTP
反制模式	SYN、UDP、TCP、ACK、IGMP、ICMP、DNS、CC
上线方式	IP/域名
启动方式	系统服务
支持平台	Windows/Linux/IoT

### 2.2.4 行业优势

- 跨平台——完美兼容 window 全系列系统上线：Windows XP/Vista/7/8/8.1/10;Windows sever 2000/2003/2008/2012/2016。同时兼容 Linux/CentOS/Ubuntu/AIX/Solaris/HP-UX 等系统和主流 IoT 物联网设备系统
- 灵活性高——系统支持智能反制功能，可根据反制目标存活状态自动选择是否进行反制。

Automatic pentesting system that supports Windows, Linux, web services, and networking equipment with support for various pentesting frameworks.



(自动化渗透测试平台运行形态图)

### 2.3.2 产品功能

- **自动化渗透：**通过对目标进行漏洞扫描、漏洞利用、权限获取等一系列流程，发现目标开放的端口及服务，根据探测到的信息，系统进行漏洞利用，进一步获取目标权限，具体内容如下：

#### a) 漏洞扫描

- 1) **漏洞快速扫描：**针对 Windows 主机、Linux 主机、Web 站点、网络设备等各类目标，进行快速扫描测试，确定主机在线状态、端口开放情况、操作系统版本等信息，并将结果生成报告。
- 2) **漏洞详细扫描：**系统内置上万种检测模板和漏洞，支持 Web 漏洞扫描、操作系统漏洞扫描、弱密码检测等功能，对被测系统所有弱点、技术缺陷或漏洞进行主动分析，并将结果生成报告包括：主机信息、漏洞评估、漏洞详情、漏洞利用、服务列表、端口信息、数据库信息、文件目录信息、扫描历史等。

## b) 漏洞利用

- 1) 漏洞验证：可根据漏洞扫描结果，自定义选择不同风险的漏洞利用模块，对目标漏洞执行渗透攻击。
- 2) 扫描结果导入：平台支持多种第三方安全扫描工具扫描结果导入和漏洞验证，自动识别并导入报告，在系统中选择对导入的主机及对应漏洞进行渗透验证，确认漏洞真实后即可攻击。支持包括：绿盟极光、启明星辰天镜、AppScan、NeXpose、Acunetix、Core Impact、Nessus、

NetSparker、Nmap 等。

- c) 权限获取：漏洞利用成功后，系统支持根据渗透结果选择一系列按照漏洞的利用方式编写的执行代码和脚本程序，实现对目标权限的获取。

It also supports specialized APT attack scenarios, including generating email templates, browser-based attacks, exploited Office document generator and more.



➤ **APT 攻击**

- a) **邮件钓鱼：**平台支持指定电子邮件发送服务器，使用 Web 网页组件克隆与伪造 Web 站点，针对伪造站点建立电子邮件内容模板，诱导目标在伪造的 Web 站点提交敏感信息，最终达到收集目标敏感信息供进一步攻击利用的目的。
  - b) **浏览器攻击：**平台支持通过 Web 网页组件建立一个自动进行浏览器检测与漏洞利用的站点，目标被诱导浏览指定的站点，浏览器漏洞利用成功后，则自动建立连接会话。
  - c) **文件漏洞攻击：**平台支持如 Office、PDF、图片等文件漏洞，生成带攻击载荷的文件。诱使目标打开或浏览文件，漏洞利用成功后自动建立连接会话。
- **Web 攻击：**平台支持对输入的 URL 进行指定范围网页的爬取，对页面使用 Web 测试模块进行测试，包括：自动测试 OWASP 列出的最新 Web 十大安全漏洞隐患、Web 服务器存在错误配置、跨站脚本攻击漏洞、本地文件包含与远程文件包含、SQL 注入漏洞、文件上传漏洞、远程代码执行漏洞或远程命令执行等漏洞。

There's also specialized hardware for tracking down WiFi devices (i.e. alert when device with WiFi's MAC address is in range) and disrupt WiFi signals and can be controlled with a dedicated smartphone.

## 2.4 WiFi 终端定位反制设备

### 2.4.1 产品简介

WiFi 终端定位反制设备是一款针对 WiFi 信号，利用定向天线的有向性，通过信号强弱确定 WiFi 设备的定位的产品。

### 2.4.2 产品功能

- **扫描 WiFi 设备：**支持扫描周边的 AP 和终端的无线信号，对其进行置顶、条件过滤和创建扫描信息快照等操作。
- **定位 WiFi 设备：**支持无线设备定位，根据 MAC 地址的信号变化进行实时告警和发现目标，语音播报当前定位的信号值并实时显示信号变化方向。定位精度小于 1 米。
- **反制 WiFi 设备：**支持主动发现 AP 和终端并跟踪其信号实施阻断，断开其网络连接。

### 2.4.3 产品参数

硬件模块	参数项	参数值
雷达设备	电池	1000mAh, 续航 8 小时
	CPU	四核 1.2GHz 64 位
	运行内存	1GB
	尺寸	240*190*40mm
	WIFI 模块数	4
	磁盘	8GB
	定位距离	>100m
	定位精度	<1m
控制手机	电池	3000mAh
	运行内存	1GB
	机身内存	8GB
	尺寸	5.5 寸

### 2.4.4 行业优势

- 覆盖距离远——采用专用功放定向天线和 WIFI 模块提供大功率无线信号，覆盖距离远。
- 定位准确——利用天线的有向性确定 WiFi 设备的方位，然后通过信号强弱确定距离的远近，实现精准定位。
- 隐蔽性强——设备便携轻巧，采用控制手机操控，隐蔽性强。

#### 2.4.5 产品图片

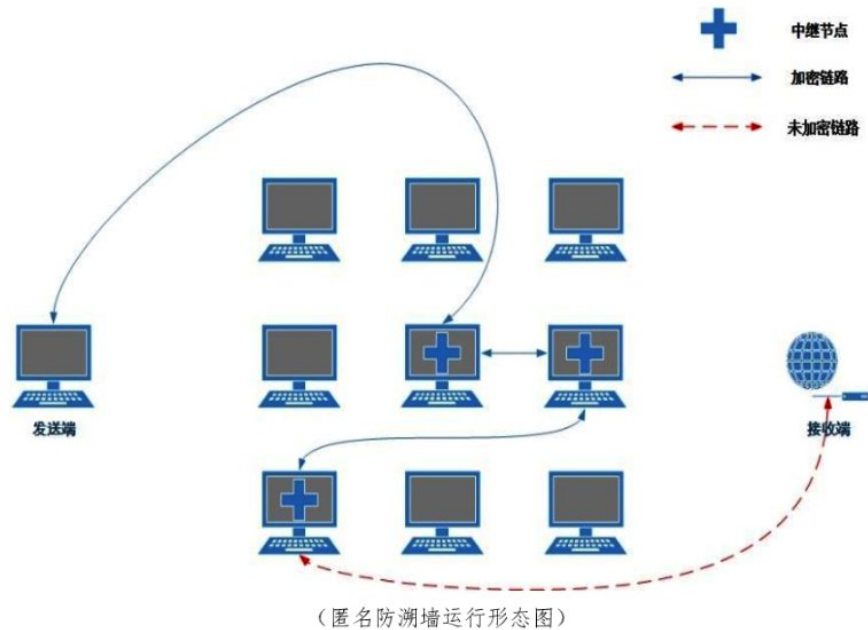


(WiFi 终端定位反制设备产品外观图)

A dedicated Tor-like device for hopping between endpoints. Designed specifically for agents working overseas.

### 3.1.1 产品简介

匿名防溯墙是安洵信息研制开发的匿名通信网络产品,用于境外网络特侦工作,通过链路强加密、多节点跳转与出口随机变化,隐藏使用者真实 IP 地址、物理地址、交互内容等敏感信息实现匿名上网功能的产品。系统能够防止敏感信息被追踪,杜绝安全风险。



### 3.1.2 产品功能

- **匿名上网:** 系统接入互联网,经过若干个中继服务器后,隐藏真实出口、真实 IP 地址、物理地址等敏感信息实现匿名上网功能。防止敏感信息被追踪。
- **端口映射:** 支持将内网终端相应服务端口映射到外围对应服务器上,实现外网访问内网相关应用的目的。可在需要接受外网回传数据等场景下使用。

### 3.1.3 产品参数

参数	匿名防溯墙
长宽高	28.2*16.1*4.3(cm)
CPU	双核 800MHz
内存	512MB DDR3
接口	4个 10/100/1000 M 自适应 LAN 口 1个 10/100/1000 M 自适应 WAN 口 4个 LAN 口灯 1个 WAN 口灯 1个 POWER 灯 1个 SYS 灯 1个 ERROR 灯 1个电源输入口
4G 上网	支持
网速	最大下载速度可达 700KB/S
中继节点	节点无上限，三次跳转
持接入设备	手机、平板、台式机电脑、笔记本电脑

### 3.1.4 行业优势

### 3.1.5 产品图片



(匿名防溯墙产品实物图)

Product stack designed for spying on users using Chinese social media, including Weibo user details lookup (email/phone), historic IP address lookup, user detail lookup via the uploaded image (i.e. Alice uploads food pic to Weibo, Alice's details can be pulled up).

## 4.1 境内舆情落查系统

### 4.1.1 产品简介

境内舆情落查系统是一套服务于实战，针对百度、新浪、天涯等多个互联网主流交互式网络平台网民注册信息实时查询的专用涉密应用系统。

### 4.1.2 产品功能

- **新浪微博信息查询：**微博链接或昵称查询手机、手机或邮箱查询微博 ID、微博历史登录 IP、微博图片溯源。
  - 1) 微博链接或昵称查询手机：通过新浪微博 URL 或昵称，可以关联其新浪微博用户的注册手机号、邮箱。
  - 2) 手机或邮箱查询微博 ID：通过手机或者邮箱号码，可以关联其新浪微博昵称或 ID。
  - 3) 微博历史登录 IP：通过新浪微博昵称，可以关联出该账户历史登录 IP、登录时间、地点。
  - 4) 微博图片溯源：通过新浪图片 URL，可以溯源其新浪微博的昵称、ID，进一步关联其账户的绑定手机号码。

Baidu lookup, reverse searching username, phone number, email address, Baidu Pan links.

- **百度信息查询：**昵称查询手机、手机或邮箱查询账户、查询知道匿名账户、百度网盘落地。
  - 1) 昵称查询手机：通过百度用户账号或昵称，可以关联其百度用户的绑定手机号码。
  - 2) 手机或邮箱查询账户：通过手机或邮箱账号，可以关联其百度用户账号或昵称。
  - 3) 查询知道匿名账户：通过百度知道匿名链接，可以关联其百度用户昵称，进一步关联其绑定手机号码。
  - 4) 百度网盘落地：通过百度网盘分享链接，可以关联其百度用户昵称，进一步关联其绑定手机号码。

Reverse searching phone number for WeChat, WeChat payment QR code, etc.

- **天涯论坛信息查询：**通过天涯用户 ID，可以关联其天涯用户的绑定手机号码，或根据手机号码关联其天涯 ID。
- **微信信息查询：**加好友二维码解析微信 ID、微信支付码解析微信 ID、手机或 QQ 号码查询微信。
  - 1) 加好友二维码解析微信 ID：通过加好友二维码关联其微信 ID。
  - 2) 微信支付码解析微信 ID：通过微信支付二维码关联其微信 ID。
  - 3) 手机或 QQ 号码查询微信：通过手机或 QQ 号码关联其绑定的微信 ID。
- **麻辣社区信息查询：**通过麻辣社区用户 tid，可以关联其绑定的手机号码。
- **QQ 部落信息查询：**提交 QQ 部落文章的链接 URL 可以关联其 QQ 部落信息。
- **运营商实名参考：**支持联通手机号的模糊姓名查询。
- **探针功能：**IP 定位、表情探针、链接探针。
  - 1) IP 定位：输入 IP，关联其 IP 定位地址。
  - 2) 表情探针：在交互式论坛发一个表情的图片链接给目标，目标打开后，获取目标的 IP、端口、时间、浏览器版本等信息。
  - 3) 链接探针：在文章里面加入超链接，目标点开 after，获取目标的 IP、端口、时间、浏览器版本等信息。

Features designed specifically for forums:

- Emote beacon: Effectively IP grabber when opened: the user's IP address, port, time, browser details are returned.

- Link beacon: Same thing as above but URL-based.

- 2) 表情探针：在交互式论坛发一个表情的图片链接给目标，目标打开后，获取目标的 IP、端口、时间、浏览器版本等信息。
- 3) 链接探针：在文章里面加入超链接，目标点开 after，获取目标的 IP、端口、时间、浏览器版本等信息。

Platform designed specifically for cracking down gambling cases, can be used to look up username, email, password, home address, IP address, etc. Notably, an email address of admin@websiteside.com can be seen. Not sure if this is a typo of "website"

## 4.2 鹞鹰反赌平台

### 4.2.1 产品简介

鹞鹰反赌平台是一款专业为相关部门设计,以打击网络赌博犯罪为目标的产品。提供网络赌博数据的挖掘、分析、研判,基于提供的数据信息,相关部门可根据数据特点和详细信息快速锁定嫌疑目标,以平台的网络赌博数据为支撑,深入开展网络赌博犯罪侦查任务,以实现网络对网络赌博组织的整体打击。

### 4.2.2 产品功能

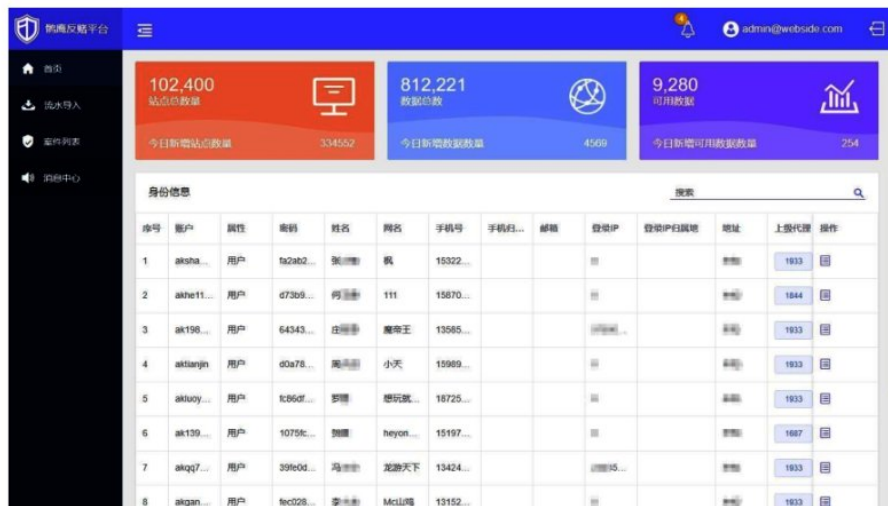
- **数据查询:** 用户可根据需求搜索相关身份信息,身份信息包括账户名、属性、密码、姓名、网名、手机号、手机归属地、邮箱、登录 IP、登录 IP 归属地、地址、上级代理等各类信息,针对可疑身份可点击操作按钮进行详细信息查看和立案操作。
- **案件管理:** 平台支持根据查询出的涉赌用户基础信息进行立案侦查和分析,结合目标账户的数据信息进行关联分析,掌握目标的上下级关系网络图谱、下线注册时间分布趋势、银行卡案值占比、下线用户地区分布、下线用户案值占比等各类信息,并支持对案件的编辑和删除功能,实现对立案账户信息的补充和完善。



#### 4.2.3 行业优势

- 数据全面可靠——平台提供全面的涉赌用户数据，为执法者提供海量涉赌人员账户数据信息，并且定期为平台数据进行更新，确保了平台涉赌数据的准确性、有效性和可靠性。
- 贴合业务场景——平台以涉赌案件业务流程进行设计，用户通过平台可实现发现可疑账户、立案侦查、综合分析溯源、到最终案件侦破，提供了完整的业务流程和案件侦破思路。
- 平台稳定可靠——平台采用 SaaS 服务为基础进行设计，平台的数据更新、维护均由专业人员进行统一管理维护，确保整套平台能够 7\*24 小时稳定运行，并且为用户提供及时的售后支持服务。

#### 4.2.4 产品图片



The screenshot displays the 'KoTH Anti-Gambling Platform' interface. At the top, there are three summary cards: '102,400 站点总数' (Total Sites), '812,221 数据总数' (Total Data), and '9,280 可用数据' (Available Data). Below these is a table titled '身份信息' (Identity Information) with columns for ID, Username, Role, Password, Name, Nickname, Phone Number, Mobile Number, Email, Login IP, Login IP Location, Address, Agency, and Action. The table lists 8 users with their respective details.

序号	账户	属性	密码	姓名	网名	手机号	手机后...	邮箱	登录IP	登录IP归属地	地址	上级代理	操作
1	aksha...	用户	fa2ab2...	张...	猴	15322...						1833	回
2	akhe11...	用户	d73b9...	何...	111	15670...						1844	回
3	ak196...	用户	64343...	庄...	魔帝王	13685...						1833	回
4	aktianjn	用户	d0a78...	高...	小天	15989...						1833	回
5	akuooy...	用户	tc86df...	黎...	想玩就...	16725...						1833	回
6	ak139...	用户	1075k...	黎...	heyon...	15197...						1687	回
7	akqj7...	用户	39fc0d...	冯...	龙腾天下	13424...						1833	回
8	akgan...	用户	fec128...	李...	McL山崎	13152...						1833	回

(鹤鹰反赌平台界面图)

They've also developed their own KoTH style CTF platform for training offsec employees.

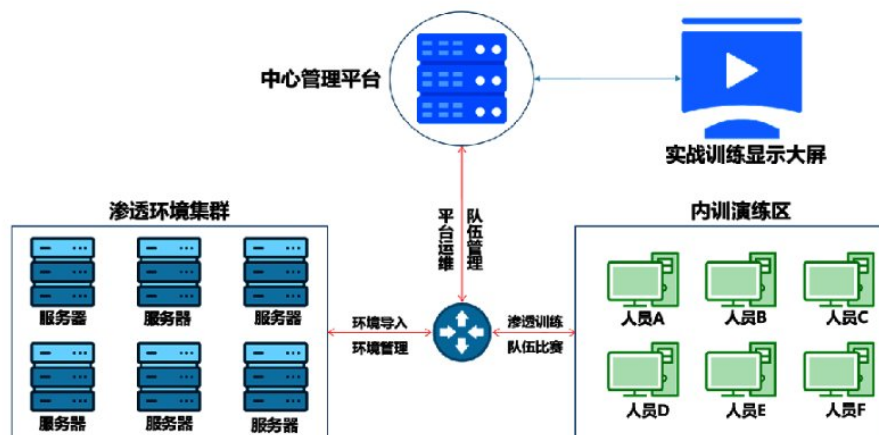
## 4.3 实战培训平台

### 4.3.1 产品简介

实战培训平台是安洵信息依托多年积累的网络安全渗透实战经验，结合各网络侦查单位对网络安全人才的技能要求，自主研发的一套专业的实战培训平台。

专业的数字情报解决方案提供商

学员可在基于实战场景 1:1 搭建的内网渗透环境中，进行真实地网络安全对抗，提高学员的实际工作能力。



(实战培训平台运行形态图)

### 4.3.3 行业优势

- 真实的内网环境——实战培训平台基于我公司多年APT渗透攻击经验总结研发，将解题模式内嵌到真实的内网环境中，学员一方面可以通过解题提交 flag，同时可以根据每一题的线索自行发现整个内网中的主机进行下一步渗透。
- 可视化仿真环境自定义——平台支持用户自定义上传环境，一方面可以进行真实的网络攻防实训，提高学员的实际工作能力；另一方面也可以在这些环境上进行新技术的科研、测试，提高本单位的网络攻防科研水平。
- 热点安全事件分析还原——实战平台可通过模拟热点安全事件真实环境，可分析还原事件，将事件中涉及到的攻防技术还原到实战中提供给学员。

### 4.3.4 产品图片



实战培训平台界面图

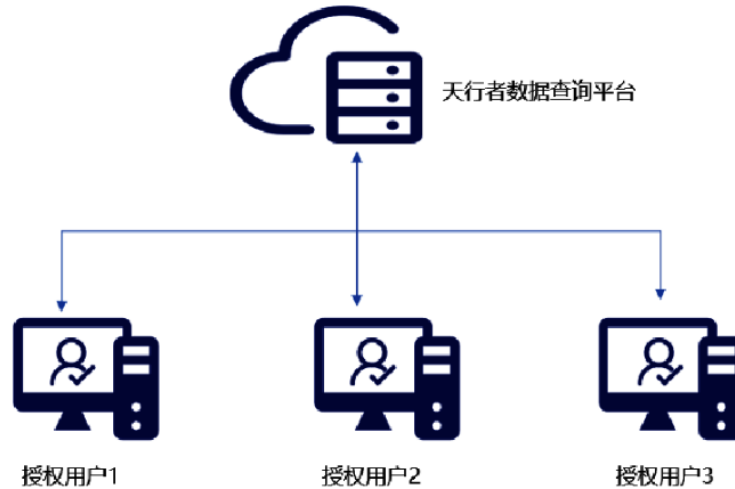
"Skywalker" data research platform. Used to look up information related to the keyword, such as phone address, email, username, which would then bring up their IRL details.

## 4.4 天行者数据查询平台

### 4.4.1 产品简介

天行者数据查询平台是一套服务针对目标物流信息、网络虚拟身份信息提供实时查询的专用涉密应用系统。平台以物流信息为支撑，同步关联目标相关信息，实现对目标人物信息的全面获取。

天行者数据查询平台基于云服务的方式提供给客户进行使用，用户通过授权加密狗即可登录到系统中，使用各个系统的功能模块。



(天行者数据查询平台运行形态图)

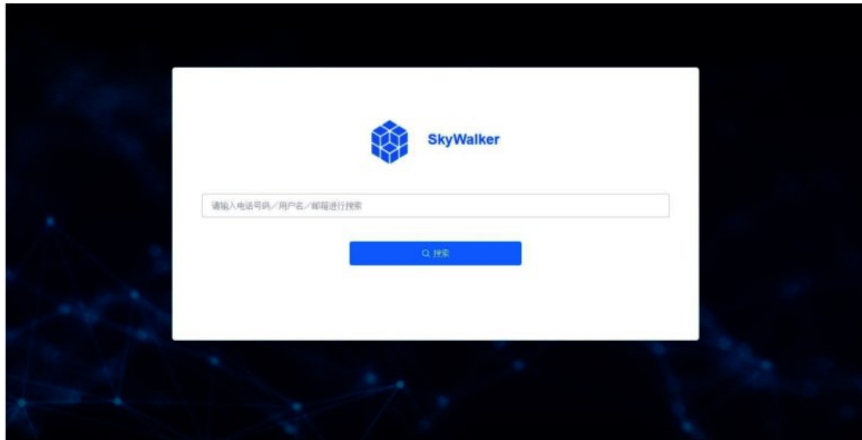
This information can then be fed into an "in-development" feature of looking up user details on various social media, including QQ, WeChat, Weibo, Facebook, and Twitter.

- **虚拟身份查询（开发中）**：在查询出目标人员信息后，可根据查询的关键字，可关联查询出目标的网络虚拟身份，包括 QQ、微信、新浪微博、Facebook、Twitter 等账号信息。

#### 4.4.3 行业优势

- 操作简单——界面简洁，易操作，按要求输入目标信息关键字即可获得查询信息。
- 数据支撑——平台内置我公司独有威胁情报数据为相关部门信息落查做支撑，用户可通过互联网实时在线查询，迅速获得返回信息。
- 安全性高——为确保查询的安全性和隐蔽性，平台在查询过程中采用了链路多层加密技术，配合 USB key 登录，确保数据查询请求和结果反馈双向通信的安全性。

#### 4.4.4 产品图片



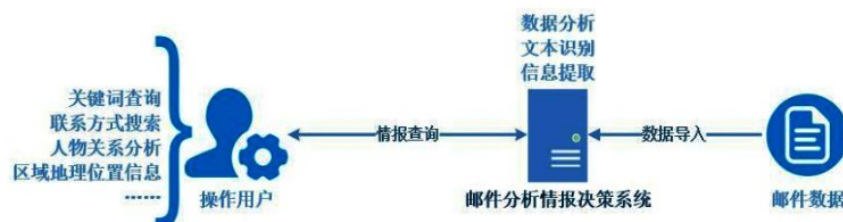
Email text search platform. The emails can be automatically imported via SMTP, POP3, iMAP, and most importantly, Exchange. Exchange server can be configure to add "non-plaintext" transfer during transport.

## 4.5 邮件分析情报决策系统

### 4.5.1 产品简介

邮件分析情报决策系统基于文本识别大数据技术研发设计,支持对海量邮件数据快速识别分析,提取关键字、敏感词、人物关系、联系方式等情报信息。

系统安装部署简单,只需将应用软件部署在服务器上,即可实现对邮件大数据的分析应用。



(邮件分析情报决策系统运行形态图)

### 4.5.2 产品功能

- **邮件自动收取:** 系统支持 SMTP、POP3、iMAP、Exchange 协议下的自动化收信; 其中 Exchange 下支持使用非明文口令进行收信。
- **全文快速搜索:** 系统支持根据时间、区域、标签等条件对不同数据源的邮件数据进行快速搜索。

That was \*most\* of the data in just ONE PDF file that is leaked from this repository. There's presumably a lot more to dig through.

The rest of the repo seems to be mostly low-res screenshots (presumably thumbnails?) of various WeChat logs, and random camera shots of random notes.

I'll be posting the rest of the updates back in the Mastodon thread.



<https://infosec.exchange/@still/111954573531369333>

This blew up so instead of plugging something I'm gonna tell you to go read the chat log analysis I'm doing over at .



<https://infosec.exchange/@still/111954573531369333>

There's also a RAT called Hector.

"Hector is an active RAT that supports HTTP/WebSocket and HTTPS/WS over TLS."

"Hector supports interactive remote shell, file directory viewing, file management."

## 第6章 使用说明

### 6.1 整体的文件结构

 Console	2019/8/1 15:14	文件夹
 Door	2019/8/5 11:49	文件夹
 tools	2019/8/7 15:47	文件夹










说明:

Console: 存放控制端程序;

Door: 存放木马配置器程序;

Tools: 存放生成 https 证书的工具;

#### 6.1.1 控制端-console

 Plug-in	2019/8/1 15:14	文件夹	
 Plug-Out	2019/8/1 10:35	文件夹	
 Engine.dll	2019/8/1 14:42	应用程序扩展	521 KB
 Engine.pdb	2019/8/1 14:42	PDB 文件	2,875 KB
 FileManager.dll	2019/8/1 11:32	应用程序扩展	213 KB
 Hector.exe	2019/8/1 14:53	应用程序	267 KB
 Hector.ini	2019/7/30 17:13	配置设置	1 KB
 Hector.pdb	2019/8/1 14:53	PDB 文件	6,715 KB
 InfoStorage.dll	2019/7/31 18:30	应用程序扩展	95 KB
 InfoStorage.pdb	2019/7/31 18:30	PDB 文件	1,435 KB
 mfc100u.dll	2019/7/22 14:08	应用程序扩展	4,320 KB
 msvcp100.dll	2019/7/22 14:08	应用程序扩展	412 KB
 msvcr100.dll	2019/7/22 14:08	应用程序扩展	756 KB
 SQLite3.dll	2019/3/22 10:21	应用程序扩展	444 KB
 terminal.exe	2014/11/21 0:00	应用程序	374 KB

说明:

Hector.exe: 控制端主程序;

Hector.ini: 控制端配置文件;



## 第3章 产品功能

- 1、通信协议：支持 HTTP/WEB SOCKET、HTTPS/WEB SOCKET over TLS 协议；
- 2、远控功能：
  - 1) 交互式 shell 命令行；
  - 2) 文件目录浏览
    - 以图形化方式查看，支持直接执行某个可执行文件；
    - 支持直接输入绝对路径浏览指定目录；
    - 支持记录最近输入的路径信息
  - 3) 文件传输
    - 文件上传、下载、运行、删除、小文件内容查看等；
    - 支持断点续传，支持暂停、启动、删除传输任务
- 3、主机管理功能：对上线主机的管理，支持分组管理、修改备注、修改组等。
- 4、主机日志：记录目标主机名、用户名、上线 IP、上线时间、下线时间、主机基本硬件信息等数据；

## 第1章 概述

Hector 远程控制系统是一套支持 HTTP/WEB SOCKET、HTTPS/WEB SOCKET over TLS 协议，采用反向连接方式的远程控制系统；

远控系统支持交互式 shell 命令行、文件管理等功能；

## 第2章 名词解释

### ➤ WEB SOCKET 协议（简称 WS）：

WebSocket 是一种网络传输协议，可在单个 TCP 连接上进行全双工通信，位于 OSI 模型的应用层。WebSocket 使得客户端和服务端之间的数据交换变得更加简单，允许服务端主动向客户端推送数据。在 WebSocket API 中，浏览器和服务器只需要完成一次握手，两者之间就可以创建持久性的连接，并进行双向数据传输。

与 http 协议的区别在于：http 协议服务端不支持主动发送请求到客户端，而 WEB SOCKET 协议可允许服务端主动向客户端推送数据；

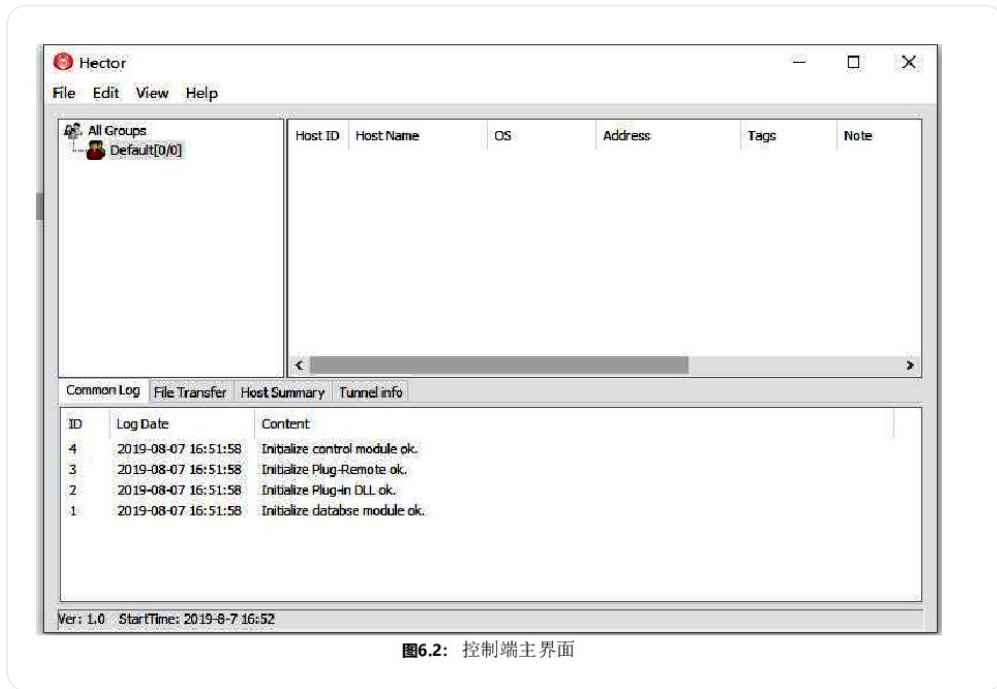


图6.2: 控制端主界面

Modular design and supports additional plugin deployment

### 7.1.1 单个插件下发的使用说明

在控制台可以单独对某台在线主机下发插件，具体步骤：

- 1、在控制台右侧主机列表中选中要下发插件的在线主机，右键单击在弹出的菜单栏中选中“Host Panel”菜单项，打开单个下发插件窗口，如图所示：

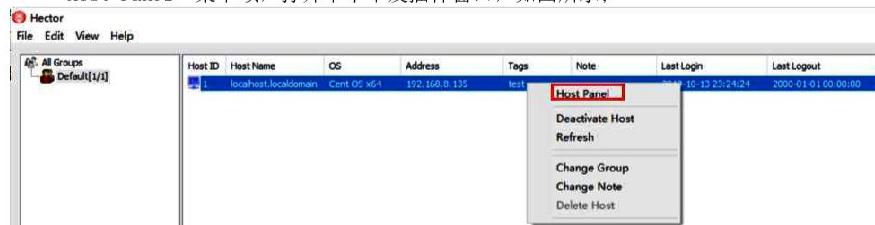


图7.1: Host panel 窗口

- 2、在单个下发插件窗口选择插件类型，单击“Update Ext”按钮，就可以为选中的在线主机下发选中的插件了

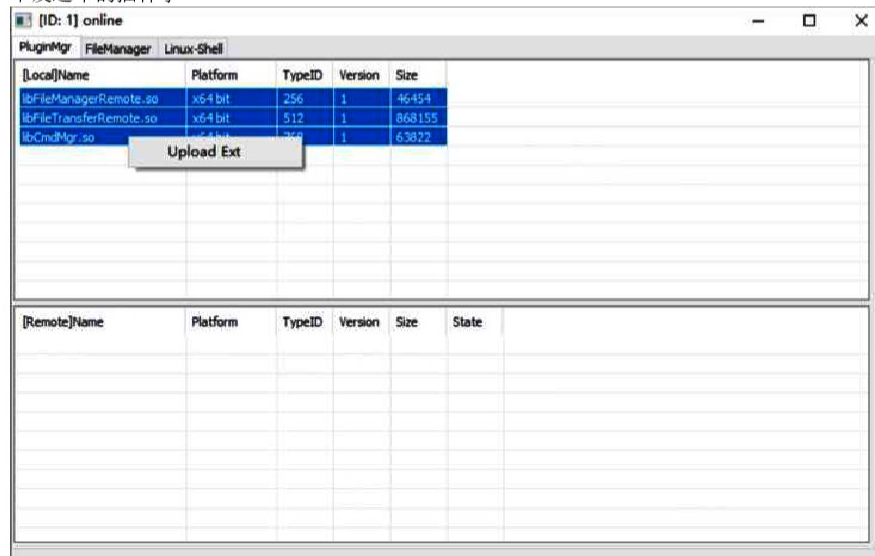


图7.2: 手动的下发插件

...