Product manual

(Ver1.0 2020)

Table of contents

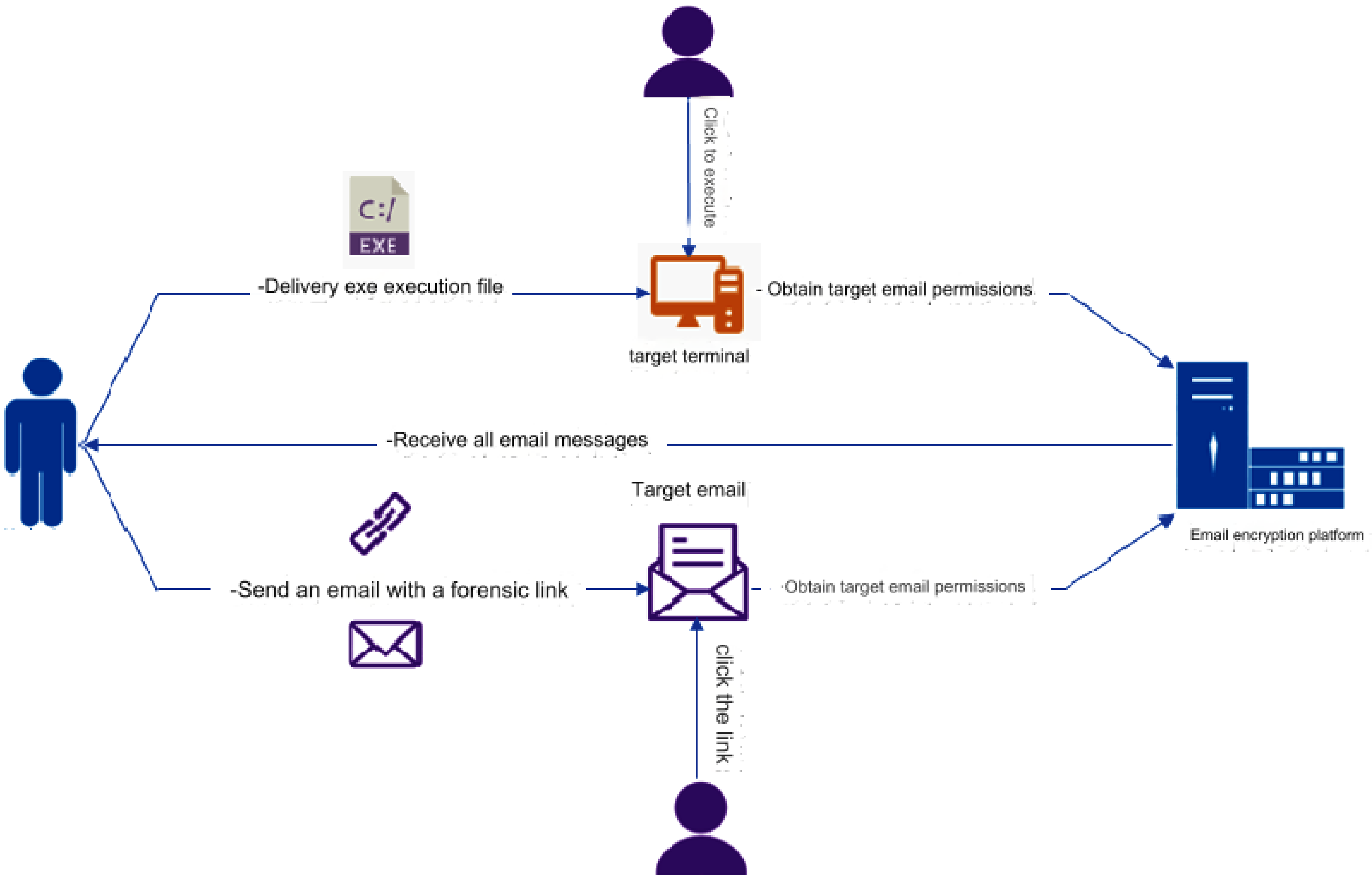
- Special control secret access type

1.1 Email encryption platform

1.1.1 Product Introduction

The email encryption platform is comprehensively developed and designed based on more than one year of research on Google/Microsoft security mechanisms.

It uses non-perception and anti-secondary verification technology to obtain the permissions of the target mailbox and achieve the acquisition of the target email content.


Click to execute
C:/
EXE
-Delivery exe execution file
- Obtain target email permissions
target terminal
-Receive all email messages
Target email
Email encryption platform
-Send an email with a forensic link
·Obtain target email permissions
click the link

(Operation status of email encryption platform)

1.1.2 Product functions

> Execution file download: Users can choose to download the corresponding forensic execution file version according to their needs, and deliver this execution file to the target terminal.

> Link generation: The platform can generate a forensic link based on the user-specified link (real or custom link), and the user can send this link to the target email address. (for Outlook mailbox evidence collection)

> Import protocol: Users can import Exchange, POP3, and IMAP protocol data based on the target mailbox situation.

> Generate GPG: The user generates the corresponding GPG Key according to the target mailbox, and performs encrypted transmission, decryption and viewing of the email.

> Mailbox acquisition: When the target clicks on the execution file/evidence collection link, the platform can obtain the target mailbox permissions, thereby obtaining the target mailbox's inbox, outbox, contacts and other email data contents.

> Task management: The platform supports the management of tasks for establishing each target mailbox. You can check the progress of each task at any time, and fully understand the task dynamics in real time, which facilitates management.

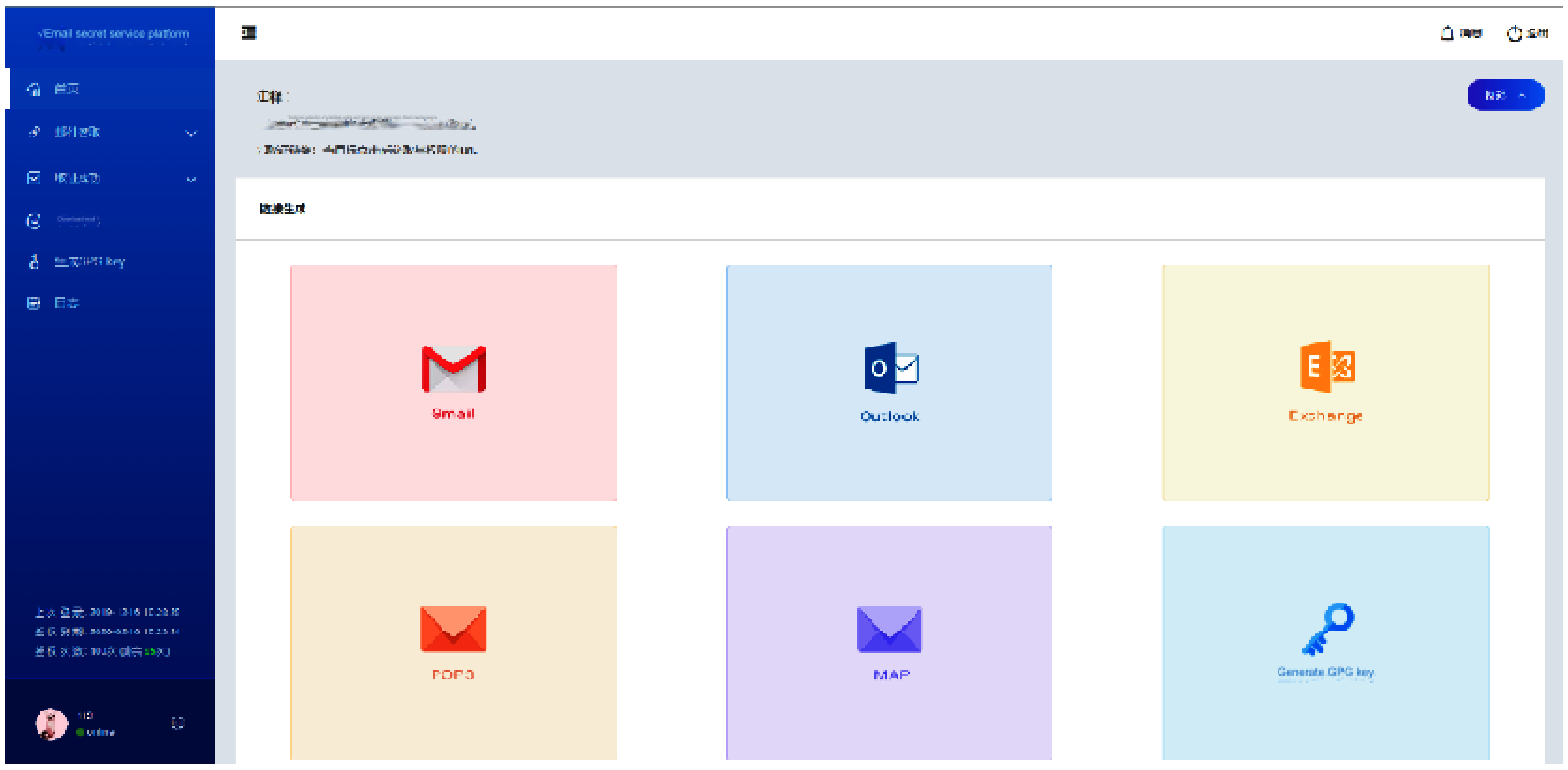
> Log records: The platform supports viewing log records to facilitate users to view operation details.

1.1.3 Industry advantages

- Non-inductive forensics——By executing the file/evidence collection link, the backend system can quickly obtain the account permissions without the target person having to enter the account password again, thus reducing the target's vigilance and defense.

- Two-step verification bypass technology——The platform can directly bypass Google/Microsoft two-step verification such as login IP and mobile phone verification code. The target does not have active perception during the whole process and obtains the target's email data.

1.1.4 Product pictures



(Interface diagram of email encryption platform)

1.2 Twitter Control Forensics Platform

1.2.1 Product Introduction

The Twitter Control Forensics Platform is a product that integrates information inquiry, countermeasures, and monitoring of Twitter account information on the overseas social platform. It uses exclusive non-inductive forensics technology and big data intelligent crawler technology to achieve comprehensive data information tracking and monitoring of Twitter accounts.

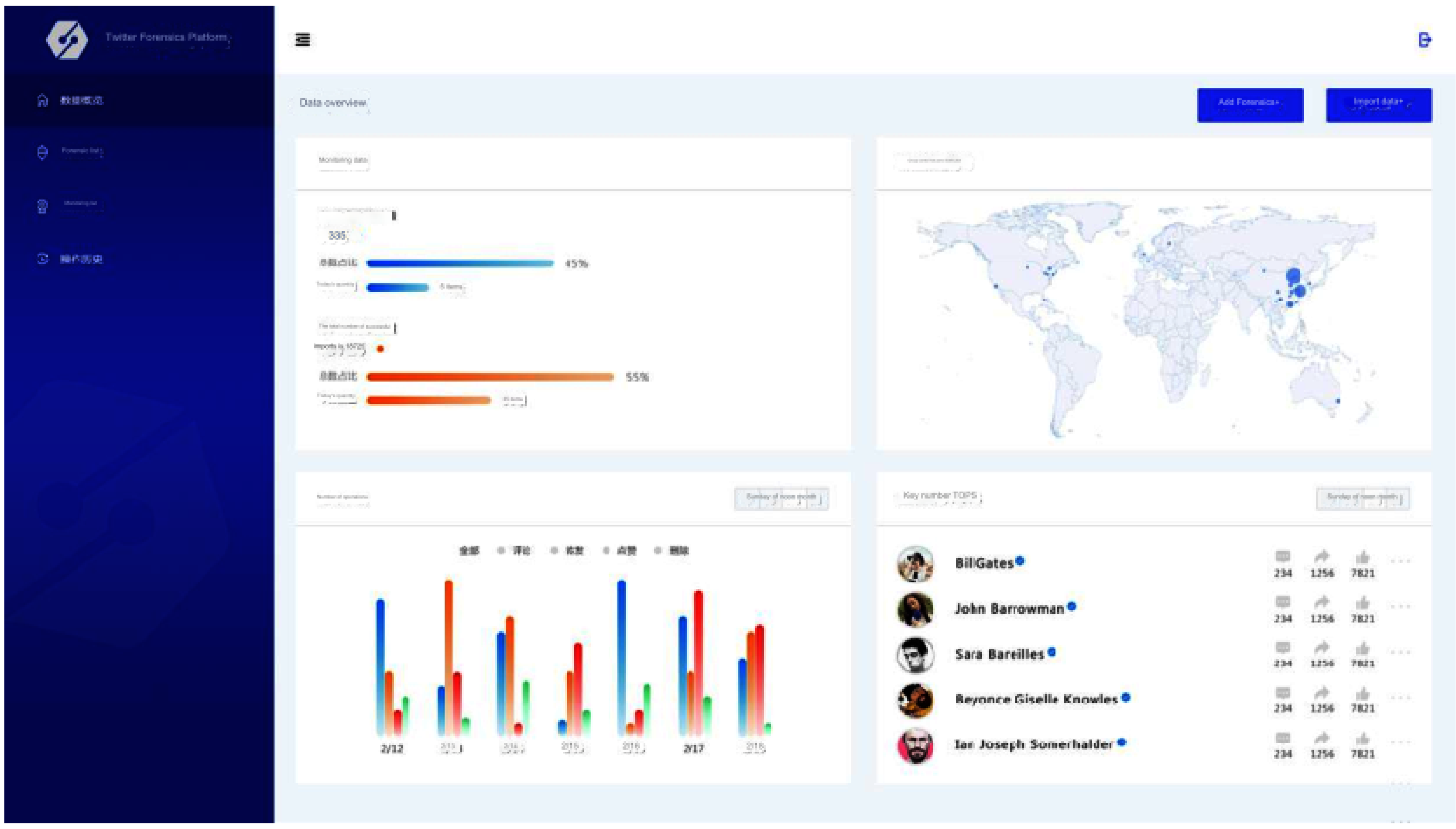
1.2.2 Product functions

- Twitter registration information query: The platform supports querying the mobile phone number and email used for registration based on the Twitter account.
- Twitter account countermeasures: The platform can generate forensic links based on user-specified links (real or custom links), send them to the target and induce them to click and perform related operations, thereby achieving the target's Twitter private message acquisition, tweet sending/deleting/ Repost/comment/like.
- Twitter account monitoring: The platform supports real-time monitoring of Twitter accounts and updates the dynamic information of the target Twitter account immediately.

1.2.3 Industry advantages

- Fast query speed——Based on the submitted target information, query results will be returned in 3-5 minutes.
- Fast data update——The-system currently runs no less than 100 million pieces of raw data every day, and supports real-time updates of available data every day.
- Unobtrusive acquisition of target information——————Through the forensic link, the background system can quickly log in to the target's Twitter account for operation without requiring the target's account and password, thus reducing the target's vigilance and defense.
- Comprehensive functions——By obtaining the permission of the target person's Twitter account, the background can directly operate the Twitter account and fully control the target person's Twitter account.

1.2.4 Product pictures



BillGates	234	1256	7821
John Barrowman	234	1256	7821
Sara Bareilles	234	1256	7821
Beyonce Giselle Knowles	234	1256	7821
Ian Joseph Somerhalder	234	1256	7821

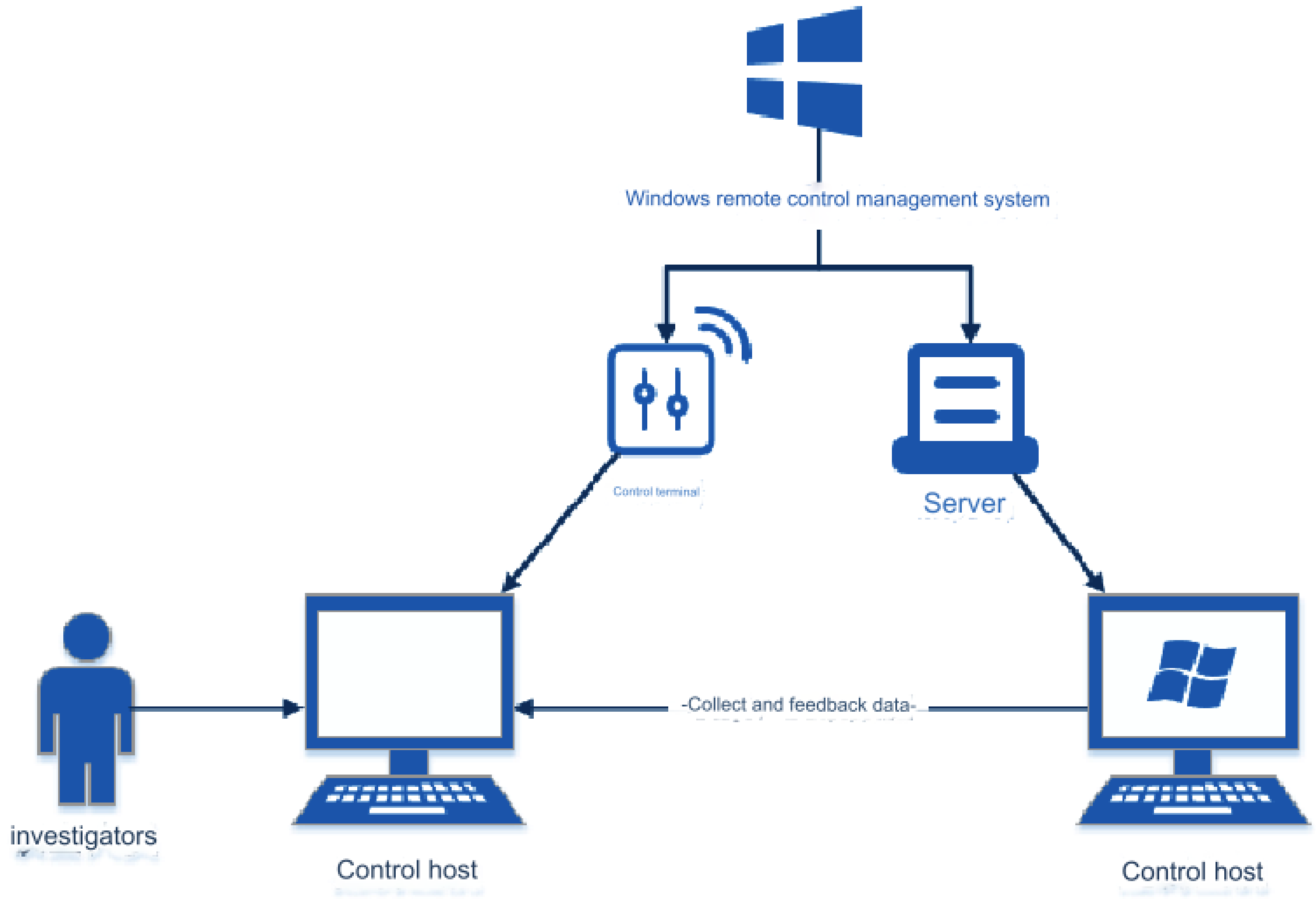
(Twitter control forensics platform system interface diagram)

1.3 Windows remote control management system

1.3.1 Product Introduction

The Windows remote control management system is independently developed based on the current mainstream network architecture and Windows system environment to realize remote operation, monitoring and evidence collection of Windows systems.

The system is mainly composed of a generator and a controller. By implanting the program generated by the generator into the target host and running it, the investigators can see the online information of the target host on the controller side, and according to the instructions of the investigators, the target The host's data is returned to investigators.


Windows remote control management system
Control terminal
Server
investigators
Control host
-Collect and feedback data-
Control host

(Windows remote control management system operation form diagram)

1.3.2 Applicable environment

operating system bits	Operating system version
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

1.3.3 Product functions

> Resource management: Supports comprehensive management of files in the target operating system.

Related files can be browsed, uploaded, downloaded, deleted, executed, renamed, etc.

> Process management: Supports real-time monitoring and control of application processes, background processes, Windows processes, etc. running on the target operating system. Including operations such as viewing, refreshing, and ending.

> Service management: Supports real-time remote management of the service status of the target operating system. Including operations such as run, pause, stop, delete, etc.

> Registry management: Supports remote management of the operating system registry. Including operations such as viewing the registry information of related programs, modifying, and deleting the registry information.

> CMD console: Supports CMD command operations on the target operating system.

> Screenshot: Supports taking screenshots of computers with target operating systems.

> Keylogging: Supports recording every key pressed by the target when operating the keyboard.

> Document access record: Supports recording of files recently accessed by the target.

▸ Online log recording: Supports recording logs of the online and offline time of the three target machines.

> Remote configuration modification: After the controlled terminal goes online, the system supports remote modification of the target machine's online address and injection of process information.

>Intranet cascading online: The system supports three ways to go online: TCP, UDP and automatic network interconnection protocol. It supports PCs in the same LAN that cannot access the Internet to go online and backhaul through PCs that can access the Internet.

> Export online host information: Supports exporting basic information of online hosts, including: online host name, internal IP address, external IP address, host memory, hard disk, CPU, network speed and other system operation and usage status information.

> Disconnect: The system has an active disconnect function. After actively disconnecting, the controlled terminal supports real-time refresh of the online domain name DNS resolution or the online IP address.

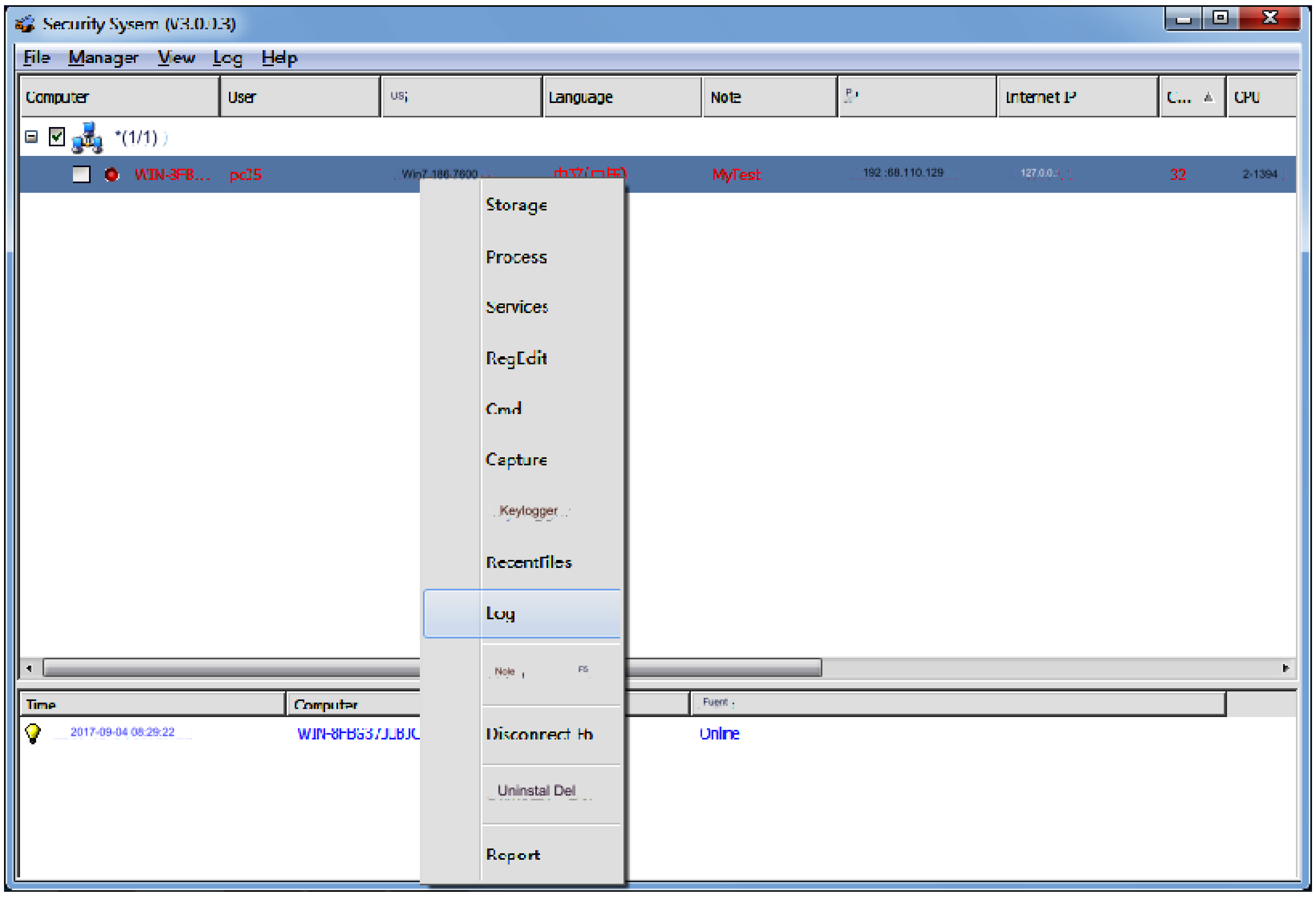
> Uninstall the server: After the control and supervision is completed, the controlled operating system supports remote uninstallation of the service.

1.3.1 Industry advantages

- High stability——The entire system is based on the new trend of remote control and adopts independent code maintenance, independent key authentication, and independent encryption algorithms to fully ensure that the control system has high stability and is not prone to offline.
- Efficient transmission——The system has a built-in independent download engine to realize extreme file transmission. It can adaptively transmit files according to the network speed. The file transmission speed can reach up to 800KB/S under 2M network bandwidth.

- Strong anti-virus protection————The system adopts the industry's unique breakthrough anti-virus active defense technology, which has strong anti-virus protection ability and can avoid detection by 95% of anti-virus software on the market, such as domestic 360, Kingsoft Anti-Virus, and Tencent Computer Manager ; Foreign mainstream anti-virus software such as Kaspersky, Symantec, and McCafé. And based on the dual technologies of storage polymorphism production and file polymorphism production, it can effectively avoid memory dynamic scanning and file static scanning protection mechanisms.
- Strong concealment - supports self-starting and self-deletion of controlled end programs after installation, and supports automatic deletion of installation files after successful installation of related programs.
- Wide applicability Supports mainstream x86/x64 Windows operating systems (including the latest Win10).
- Good ease of use——The entire system has a simple interface and simple operation, making it easy for users to get started quickly.

1.3.5 Product pictures



Computer	User	US;	Language	Note	P	Internet IP	C...	CPU
WIN-3FB...	pc25	Win7 186 7600	中文(中国)	MyTest	192 :68.110.129	127.0.0.:	32	2-1394

Time	Computer	Fuent :
2017-09-04 08:29:22	WIN-8FBG37JJBJC	Online

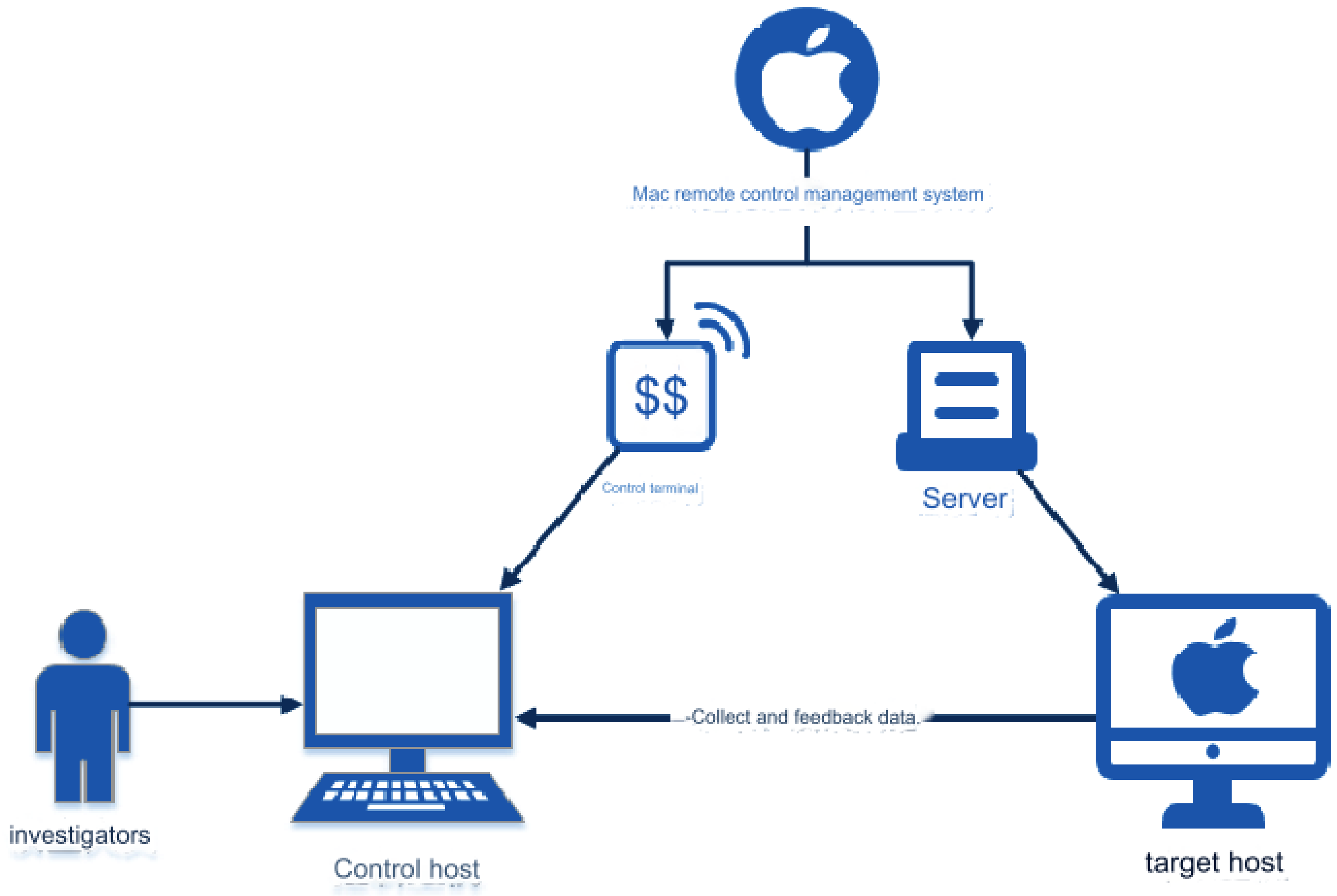
(Windows remote control management system interface diagram)

1.4 Mac remote control management system

1.4.1 Product Introduction

The Mac remote control management system is a product for Apple computer systems that implements functions such as remote file management, screen monitoring, and keylogging.

The system consists of two parts: the control end and the server end. The control end adopts a C/S architecture. The user sends control instructions to the target computer through the control end. The server end receives the instructions and executes the user's control operations on the target computer.


Mac remote control management system
$$
Control terminal
Server
investigators
Control host
Collect and feedback data
target host

(Mac remote control management system operation form diagram)

1.4.2 Applicable environment

program	Supported operating systems
Control terminal	Fully compatible with Windows NT, Windows2000, Windows XP, Windows 2003 VISTA, Windows7 and other operating systems
Server	Compatible with all versions of Apple operating system

1.4.3 Product functions

> Information management: The console interface supports displaying the computer name, user name, operating system kernel and currently released version information on the target Mac.

> File management: Supports operations such as creating, uploading, downloading (supporting breakpoint resumption), deletion, and renaming of files on the target computer.

➢ Shell command: Supports Shell command operations on the target computer.

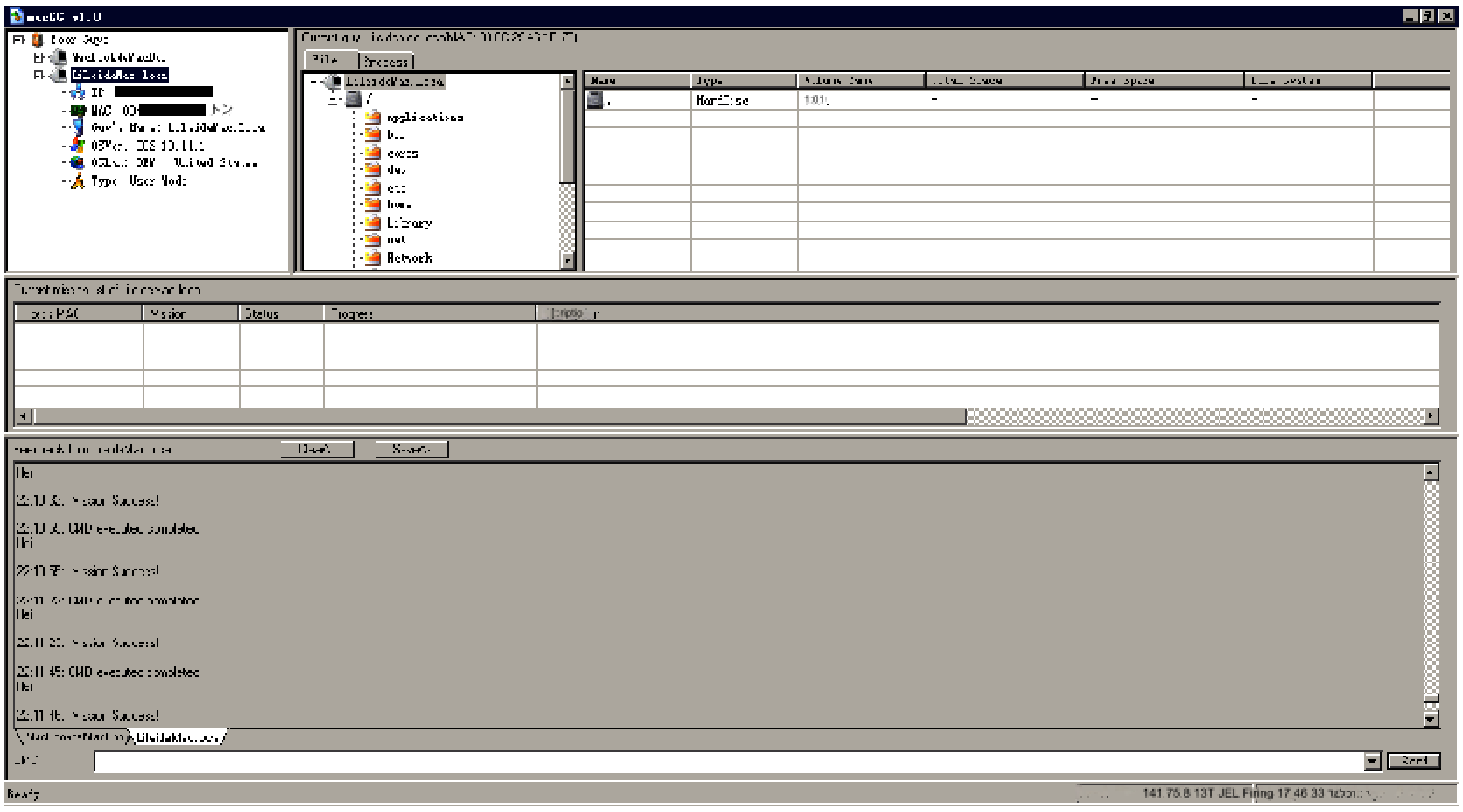
> Screenshot: Supports taking screenshots of the target computer.

> Keylogging: Supports recording every key pressed by the target when operating the keyboard.

1.4.4 Industry advantages

- Strong concealment——The server has no startup items after being implanted into the target computer, ensuring that the target computer is unaware of the entire process.
- Strong compatibility——Compatible with all versions of Apple operating system.
- High stability——The system supports 24-hour uninterrupted operation and has a self-recovery fault-tolerant mechanism.
- Fast transmission and evidence collection————When the network between server and client is 10M, the file download speed is ≥200Kb/S, the file upload speed is ≥100Kb/S, and the screen capture speed is ≥5 frames/min.
- High connection index——The maximum number of connections is ≥2000, and the system can still work normally when 100 servers are connected concurrently.

1.4.5 Product pictures



IP [redacted]

MAC 00[redacted]

Type User Mode

applications

Library

Network

Status

CMD executed completed

Success!

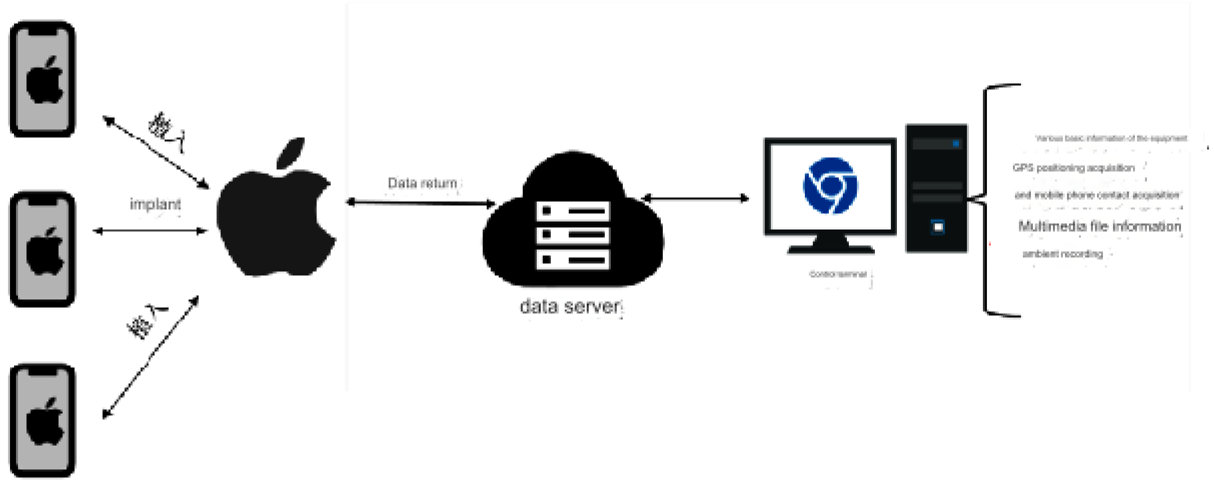
Ready

(Mac remote control management system interface diagram)

1.5 iOS remote control management system

1.5.1 Product Introduction

The iOS remote control management system is a remote information acquisition system specifically designed for iPhone devices running the iOS system to be installed without jailbreak. It can realize remote evidence collection and monitoring of iOS devices.


植入
implant
植入
Data return
data server
Control terminal
Various basic information of the equipment
GPS positioning acquisition
and mobile phone contact acquisition
Multimedia file information
ambient recording

(iOS remote control management system operation form diagram)

1.5.2 Applicable environment

model	system
All iPhone models	iOS full version

1.5.3 Product functions

> Obtain basic mobile phone information: Obtain the unique identifier, IP address, MAC address, and device version information of the target iOS system device.

> GPS positioning acquisition: regularly obtain the GPS positioning information of the target iOS system device.

> Mobile phone contact acquisition: Obtain the address book contacts of the target iOS system device.

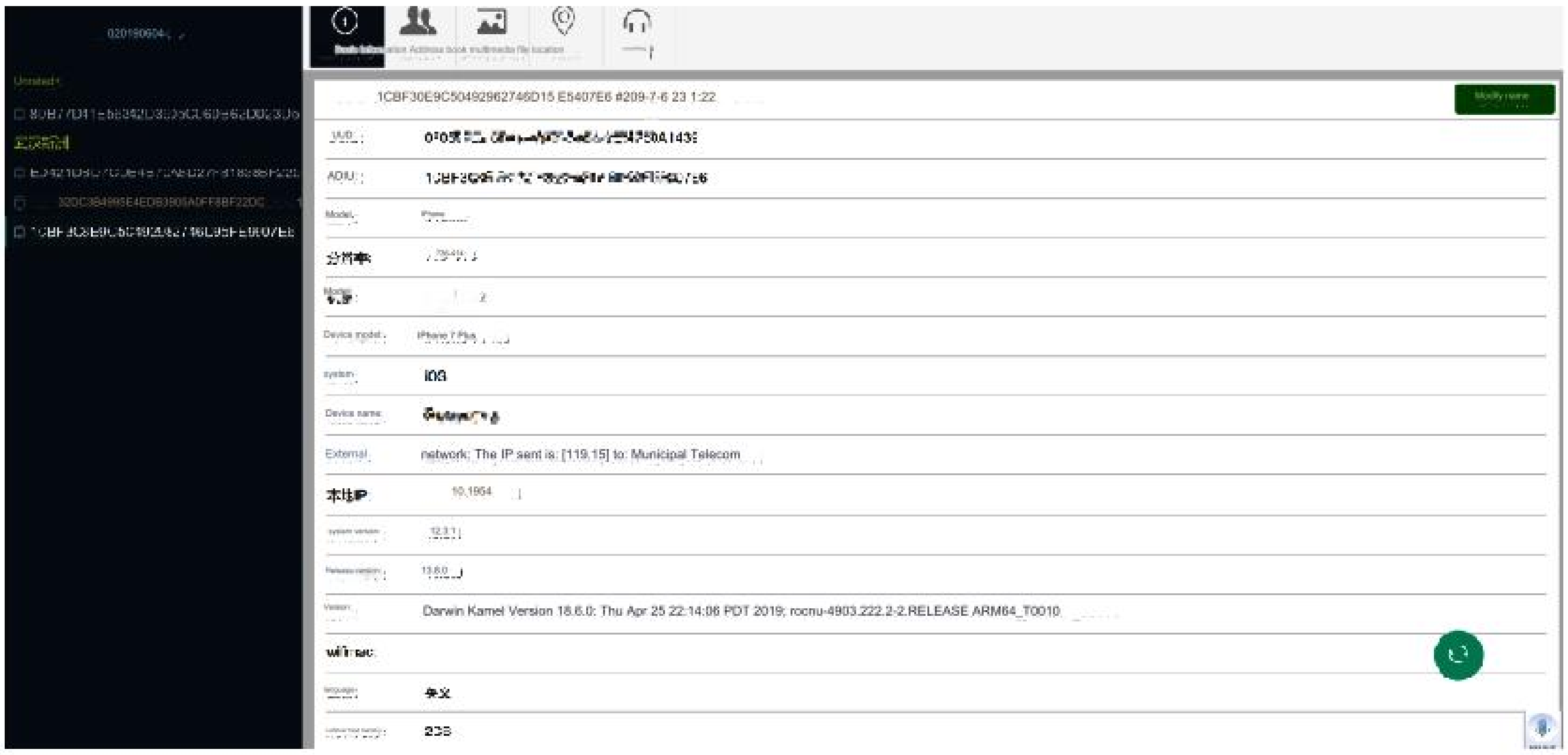
> Multimedia files: Obtain the multimedia file information of the target iOS system device.

> Recording: Supports regularly obtaining environmental recordings of target iOS system devices.

1.5.4 Industry advantages

- Jailbreak-free——Innovative way to embed the control system into the device and obtain the target data information without jailbreak.
- Strong compatibility————Compatible with a full range of smart hardware devices under the iOS system.
- Industry-leading—Being the first in the country to launch a remote control management system for iOS systems, it can be used in actual combat in conjunction with relevant law enforcement department business scenarios to achieve the acquisition of target iOS system device data information.

1.5.5 Product pictures



020190604

Unrated

□ 80B77D41E8E342D3D5C6D9E62DD23D

E3421D9D7DE4E7DAED27F8188BF22D

□ 32DC3B4998E4EDB3905A0FF8BF22DC

□ 1CBF3C3E9C5C492962746D95FE9E07E8

Basic Information Address book multimedia file location

1CBF30E9C50492962746D15 E5407E6 #209-7-6 23 1:22

Modify name

UUID: [illegible]

ADIU: [illegible]

Model: Phone

分辨率: [illegible]

Mode 信号: [illegible]

Device model: iPhone 7 Plus

system: iOS

Device name: [illegible]

External network: The IP sent is: [119.15] to: Municipal Telecom

本地IP: 10.1954

system version: 12.3.1

Release version: 18.6.0

Version: Darwin Kamel Version 18.6.0: Thu Apr 25 22:14:06 PDT 2019; rocnu-4903.222.2-2.RELEASE ARM64_T0010

wifi mac:

language: 中文

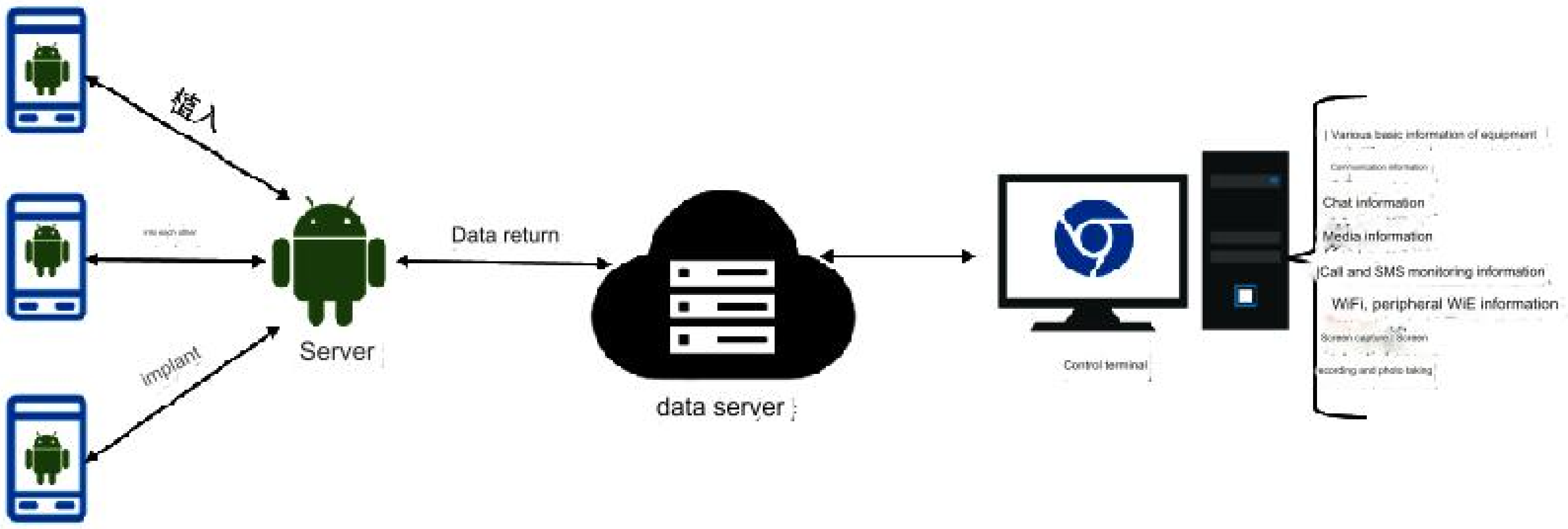
233

(iOS remote control management system interface diagram)

1.6 Android remote control management system

1.6.1 Product Introduction

The Android remote control management system realizes remote extraction of electronic data based on remote control technology. The system consists of two parts: the control end and the server end. The control end adopts B/S architecture. The server end can be installed on a variety of mainstream Android devices. After the installation is completed, it will automatically go online to connect to the control end. The server supports no less than 200 remote control systems. carry.



植入
into each other
implant
Server
Data return
data server
Control terminal
Various basic information of equipment
Communication information
Chat information
Media information
Call and SMS monitoring information
WiFi, peripheral WiE information
Screen capture, Screen
ecording and photo taking

(Android remote control management system operation form diagram)

1.6.2 Applicable environment

type	project

operating system	Android 6.0 and above
Mobile phone brands	Samsung, Xiaomi, Redmi, Huawei and other mainstream mobile phones
SIM card	Telecom, China Mobile, China Unicom
Network Type	2G、3G、4G、WiFi

1.6.3 Product functions

> Device information: Supports obtaining basic information of the mobile phone and switching on and off the mobile network of the target mobile phone. These include: device name, mobile phone model, battery capacity, system version, MAC address, phone number, mobile phone serial number, system customizer, CPU information, motherboard information, running memory, network type, IMSI, IMEI.

> Positioning information: adopts triple positioning method of network, base station (with network and card), and GPS. Supports continuous positioning, returns positioning information according to set time intervals, and supports statistics, analysis, and export.

> Contacts: Supports obtaining mobile phone contacts, supports forging targets to edit and send deceptive text messages to their contacts (valid in versions prior to Android 4.4), supports intercepting incoming calls and text messages from specified numbers (may not be possible in Android 4.4 and above) interception, some mobile phones will have sensing).

> Call records: Supports obtaining mobile phone call records, and supports statistics, analysis, and export.

> SMS: Supports obtaining SMS messages, and supports statistics, analysis, and export.

> Acquisition of various chat information: Supports acquisition of contacts and chat records on mobile phones including WeChat, QQ, and Momo chat software. (requires root)

> File management: Supports obtaining the file directory structure and file list of the target mobile phone. It can display multimedia information and quantity statistics such as music, videos, pictures, documents, etc. in categories, and supports downloading.

> Network traces: Supports obtaining traces of the network browsed by the target mobile phone's built-in browser. The obtained results can be filtered and queried by browser, time period, and title keywords. (Android 6.0 or earlier)

> Software list: Supports obtaining installed software information on the target mobile phone and account information on the mobile phone.

> Process list: Supports obtaining information about running processes on the target phone, and filtering and querying the obtained process information.

> Environmental recording: Supports environmental recording on mobile phones and mobile phone call recording.

> Camera: Supports taking photos of the surrounding environment of the mobile phone for evidence collection, including: single photo, time period photo, scene photo, front and rear camera photo.

▸ WiFi information: Supports disconnecting or connecting to the mobile phone's WiFi, and scans the visible WiFi hotspot information in the current environment of the mobile phone, including: SSID, MAC address, signal strength, password (root required), encryption method.

> Mobile phone screenshot: Supports taking screenshots of the current screen status of the mobile phone. Screen capture methods include: single Screenshots, app screenshots, and time period screenshots.

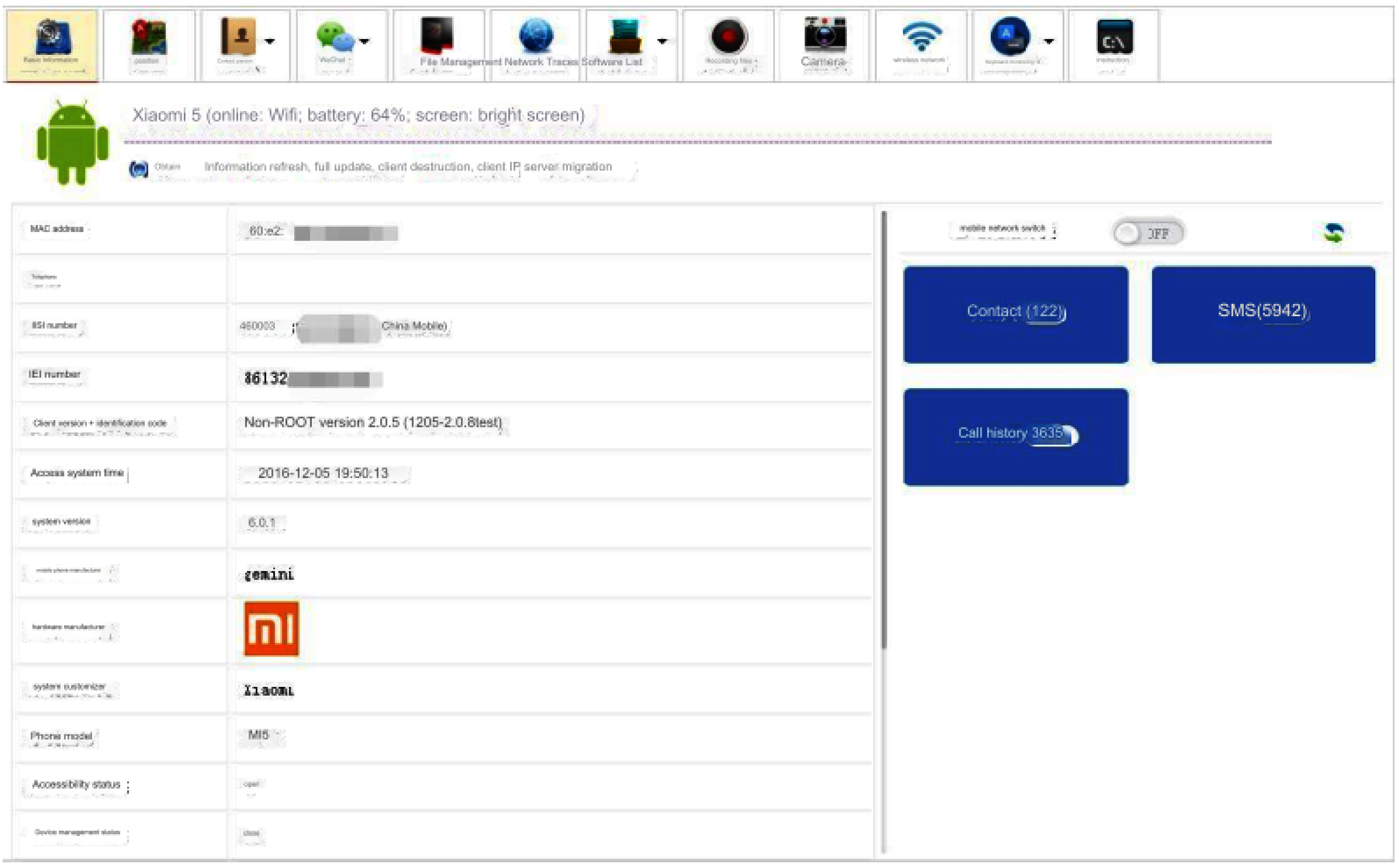
> Keyboard monitoring: Supports intercepting text messages entered by mobile phones when using QQ, WeChat, Momo, and Telegram applications. (The memory cleaning service needs to be turned on and is valid for Android 4.2 and later versions)

> System settings: Supports management command operations such as command status viewing, command sending (plan formulation), and command plan viewing for all operating commands in the system.

1.6.4 Industry advantages

- Strong compatibility——Supports most mainstream Android mobile phones on the market, such as Samsung, Xiaomi, Huawei, vivo, OPPO and other models.
- High concealment——No icon will be generated after the program is installed. When extracting various types of information, it will be extracted without any sense and no traces of operations will be displayed.
- Strong persistence supports promotion to system APP (ROOT permission required). Even if the Android device reinstalls the system, the program will still exist.

1.6.5 Product pictures



Xiaomi 5 (online: Wifi; battery: 64%; screen: bright screen)

Information refresh, full update, client destruction, client IP server migration

MAC address	60:e2: [redacted]
Telephone	
ISI number	460003 [redacted] China Mobile)
IEI number	86132 [redacted]
Client version + identification code	Non-ROOT version 2.0.5 (1205-2.0.8test)
Access system time	2016-12-05 19:50:13
system version	6.0.1
mobile phone manufacturer	gemini
hardware manufacturer	mi
system customizer	Xiaomi
Phone model	MI5
Accessibility status	open
Device management status	close

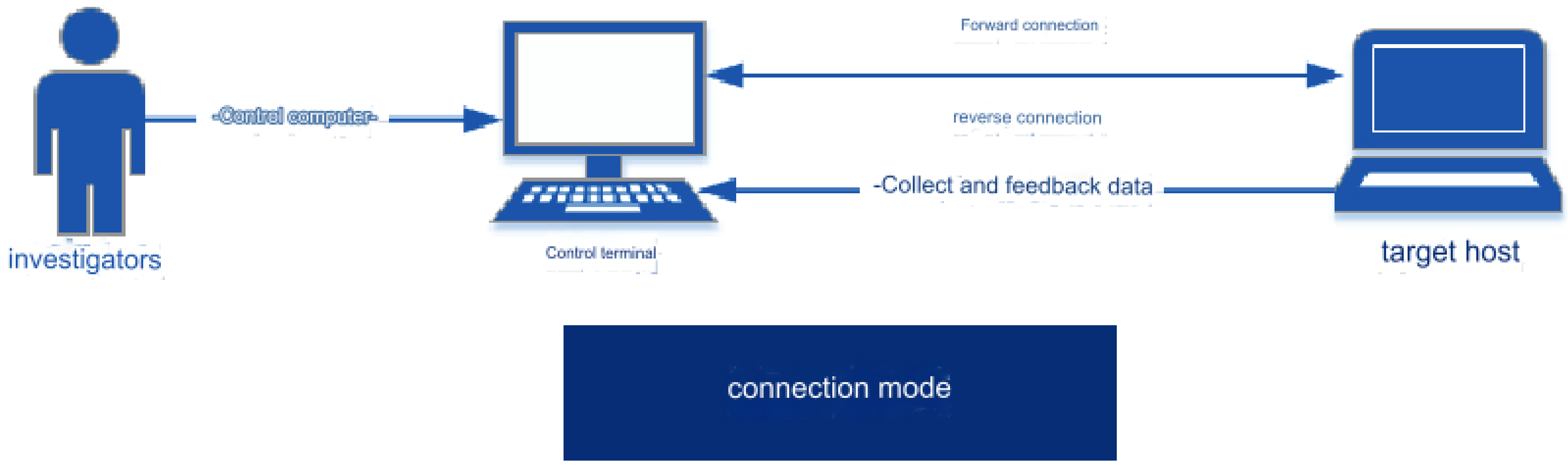
(Android remote control management system interface diagram)

1.7 Linux remote control management system

1.7.1 Product Introduction

The Linux remote control system is a system for Linux systems that can remotely control and obtain device information.

The system mainly installs the set server on the target host, and controls the target host through the operation of the control end after going online. Supports two online modes: forward connection and reverse connection.



(Linux remote control system operation form diagram)

1.7.2 Applicable environment

program	operating system bits	Operating system version
Controlled terminal (client)	x86/x64	Centos 5
		Centos 6
		Centos 7
	x64	Ubuntu 12
		Ubuntu 14
Control terminal	Windows XP/7/8, Windows Server 2003/2008, supports multiple language environments	

1.7.3 Product functions

> Shell command: You can execute Shell command operations on the client on the control terminal Shell interface.

> File management: On the remote management interface, you can view, delete, upload, download and other operations on the files and directories of the target computer.

➢ Socks5 proxy: The system supports using the SocksCap64 tool for socks5 proxy, and also supports viewing the Socks5 proxy information of the controlled end.

> TCP port reuse: The system supports communication on open ports. It only performs character matching on the input information and does not perform any interception or copying operations on network data to realize the function of port reuse.

1.7.4 Industry advantages

● High compatibility——The system supports cascading technology and supports ICMP\TCP\UDP three methods for transmission.

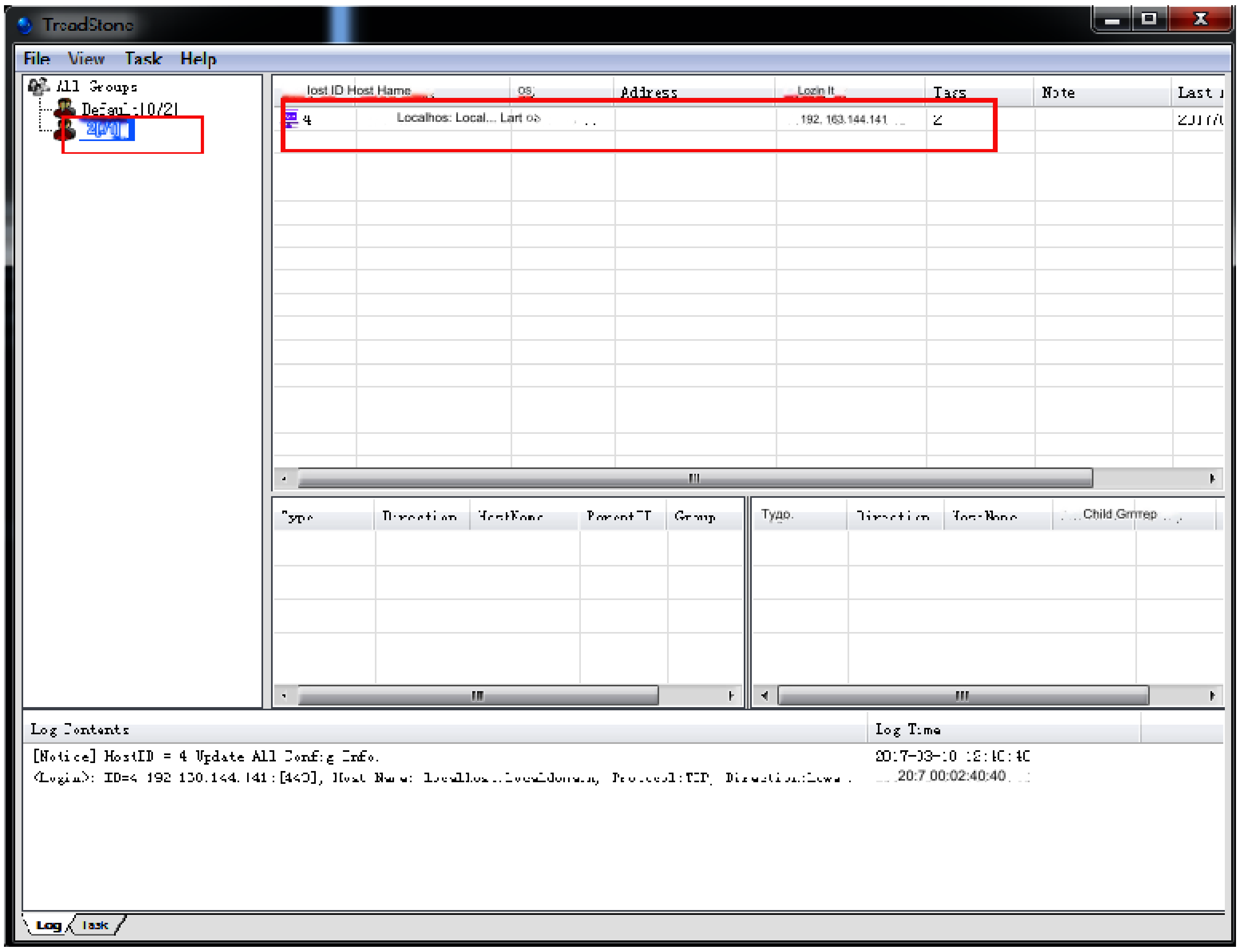
● High stability——The system supports 7*24 hours stable operation and has a self-recovery fault-tolerant mechanism.

● Strong concealment————Supports reuse of TCP ports and reserves backdoors for remote control systems.

● Good ease of use——You can choose different online modes (direct connection mode or rebound mode) according to the particularity of the target network environment to set up the second line of the client.

● Strong anti-virus software——Regular testing of domestic and foreign anti-virus software to ensure the normal use of tools. It can be anti-virus software for domestic and foreign mainstream anti-virus software, such as AVG\Clam\Comodo\Kaspersky and other mainstream Linux systems antivirus software.

1.7.5 Product pictures



lost ID	Host Hame	OS	Address	Lozin It	Tags	Note	Last
4	Localhos: Local...	Lart os		192. 163.144.141	2		2017/

Type	Direction	HostName	ParentIT	Group

Type	Direction	HostName	Child Group

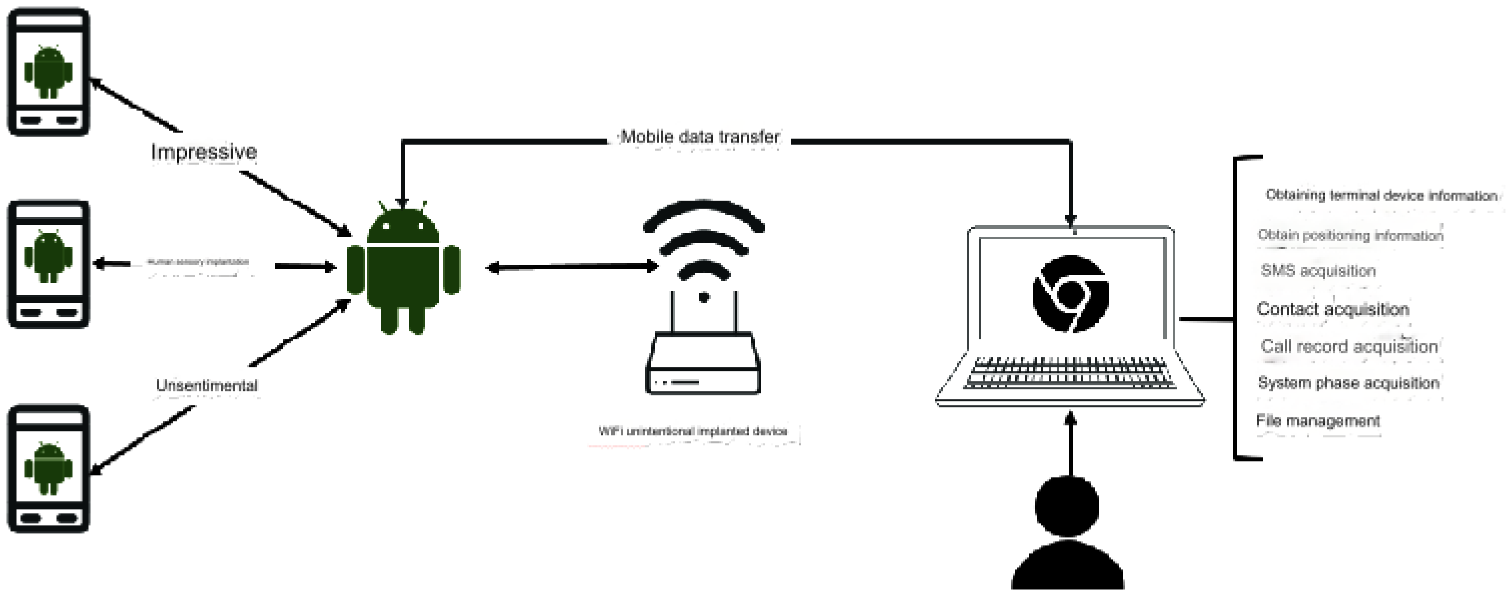
Log Contents	Log Time
[Notice] HostID = 4 Update All Config Info.	2017-03-10 12:40:40
<Login>: ID=4 192 130.144.141:[443], Host Name: localhost.localdomain, Protocol:TCP, Direction:Lowe .	20:7 00:02:40:40

(Linux remote control system interface diagram)

1.8 WiFi sensorless implantable device

1.8.1 Product Introduction

The WIFI sensorless implant device is a portable hardware device that implements sensorless implantation of specific software for Android terminals connected to the device's WiFi. After the implant is installed, key data in the terminal device can be automatically obtained and displayed visually.



(Operation form diagram of WiFi sensorless implanted device)

1.8.2 Product functions

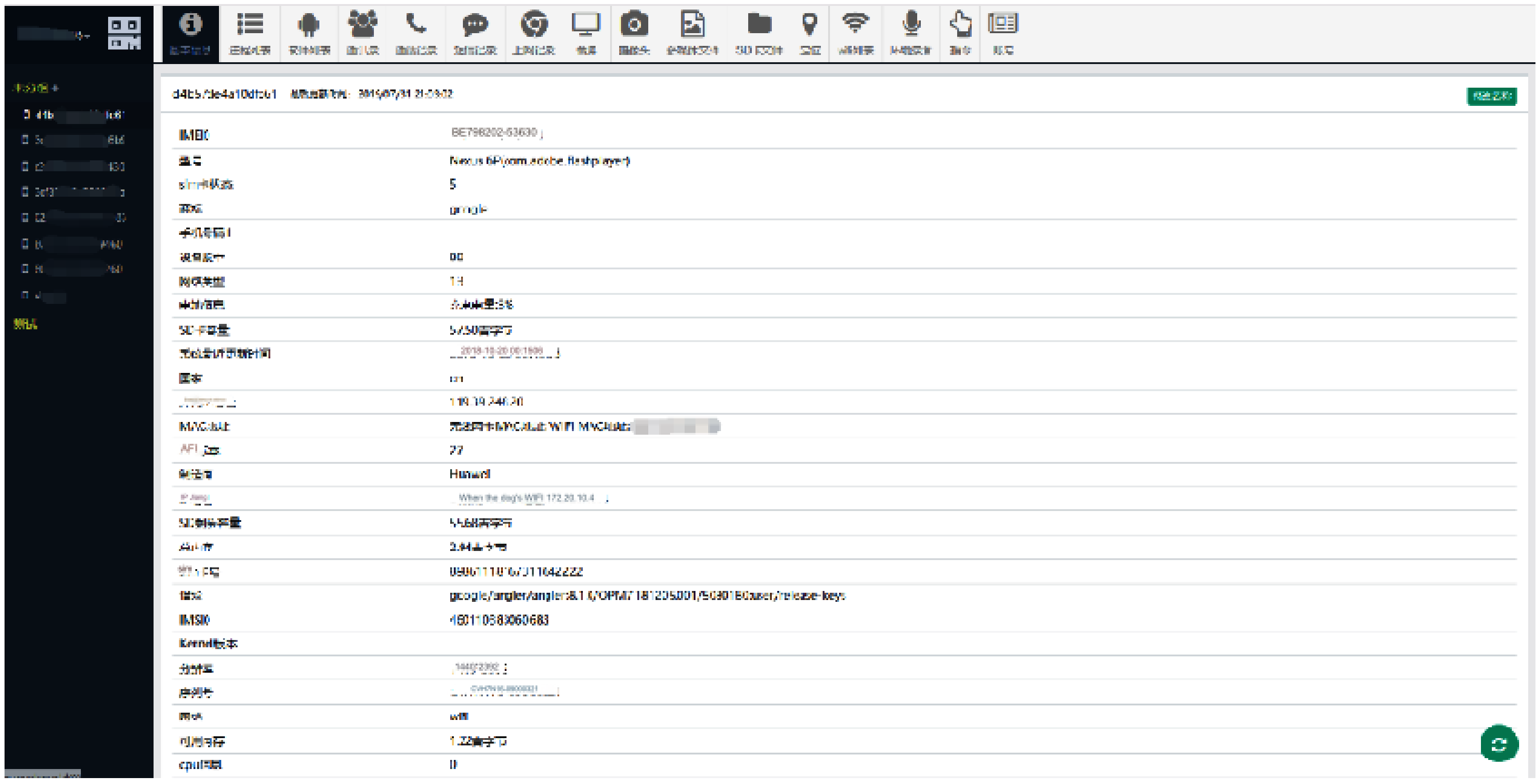
> Senseless implantation: The device supports senseless implantation using mainstream software. You only need to connect to the WiFi released by the device and then use the software regularly, and the implantation can be completed without any sense.

> Data acquisition: After successful implantation, terminal device information, positioning information, text messages, contacts, call records, system albums, and file management can be obtained.

1.8.3 Industry advantages

- High portability——The implanted device is small and portable, can be carried around, plug and play, and supports 3G/ 4G and wired connection to the Internet.
- High ease of use. The implantation process is simple. Just connect the implanted device to WiFi and access the Internet normally. No unnecessary operations are required. There are no pop-up reminders, reducing the target's vigilance.

1.8.4 Product pictures



d4eb7de4a10dfc61 最后更新时间: 2019/07/31 21:03:02

IMEI	BE798202-53630
型号	Nexus 6P(com.adobe.flashplayer)
sim卡状态	5
品牌	google
手机号码	
设备版本	00
网络类型	13
电池信息	[illegible]电量:5%
SD卡容量	57.50亿字节
[illegible]	2018-10-20 00:1000
国家	cn
[illegible]	119.39.246.20
MAC地址	无线网卡MAC地址 WIFI MAC地址: [redacted]
API 版本	27
制造商	Huawei
IP 地址	When the dog's WIFI 172.20.10.4
SD卡剩余容量	55.68亿字节
总内存	2.84亿字节
[illegible]	0900111010673110642222
指纹	google/angler/angler:8.1.0/OPM7.181205.001/5080180:user/release-keys
IMSI	460110383060683
Kernel版本	
分辨率	1440*2392
序列号	[illegible]
网络	wifi
可用内存	1.22亿字节
cpu[illegible]	0

(WiFi sensorless implant management backend interface diagram)

2. Attack Countermeasures

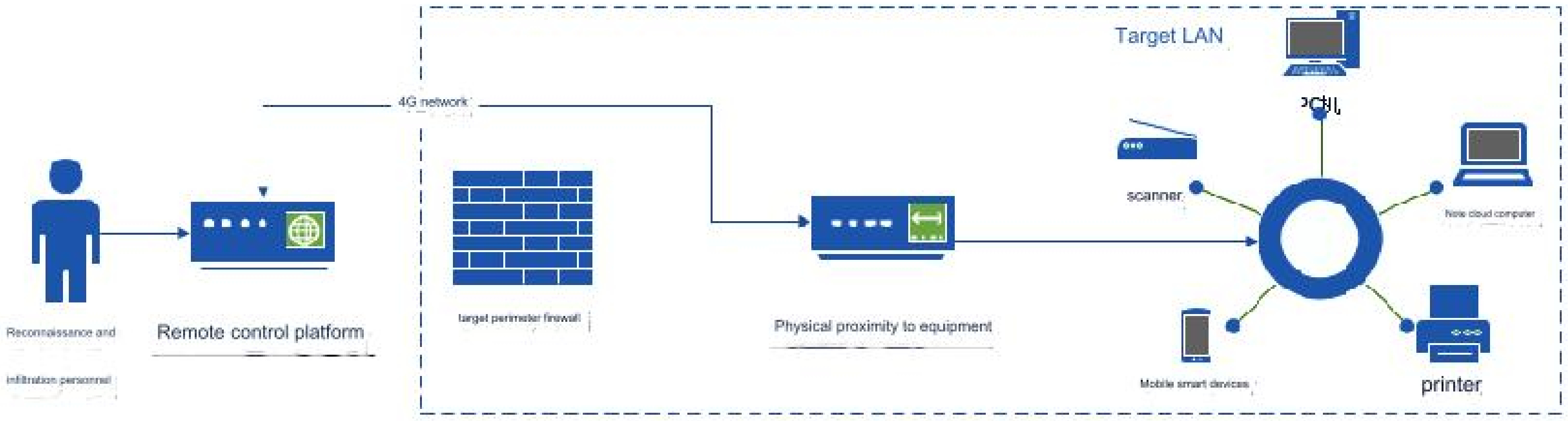
2.1 WiFi proximity attack system

2.1.1 Product Introduction

The WiFi proximity attack system is developed based on the penetration idea of near-field proximity attack, achieving the purpose of remotely controlling proximity devices to penetrate the target intranet, and improving the concealment, convenience and accuracy of penetration.

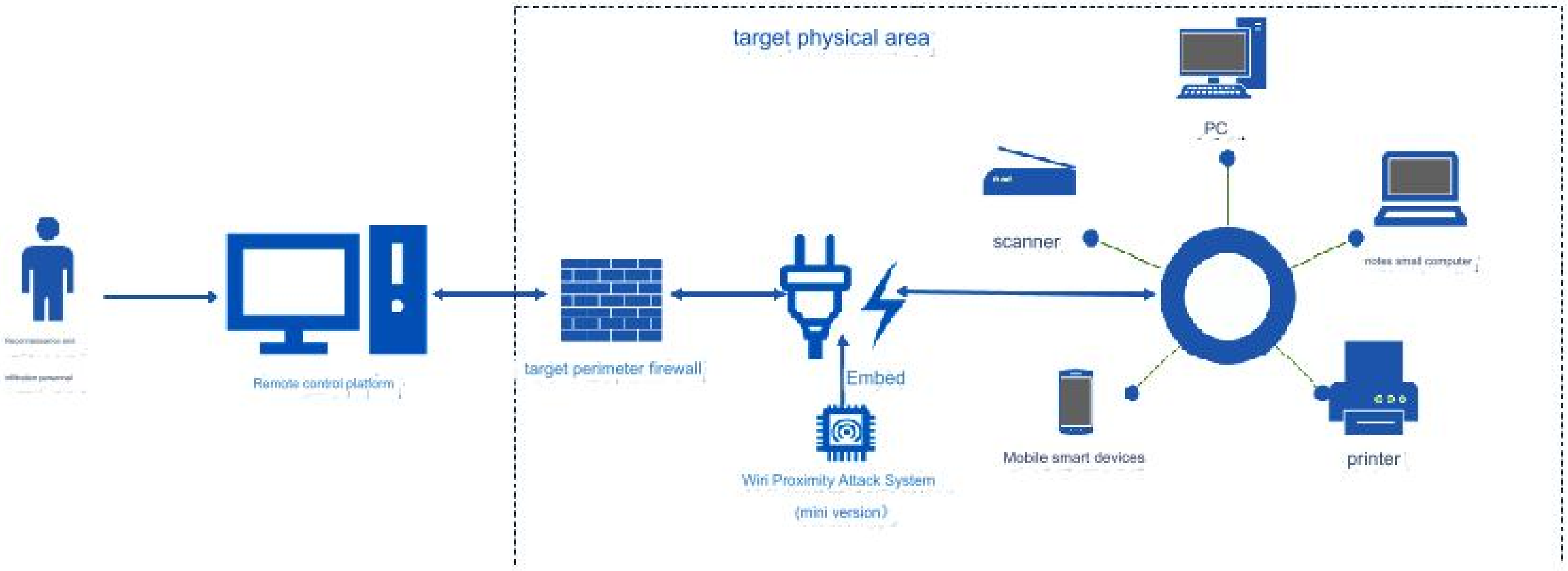
The entire system is divided into two versions, including: WiFi proximity attack system (basic version) and WiFi proximity attack system (mini version).

The basic version of the system adopts an architecture design that combines far and near ends. The remote control platform is deployed on the public network server and is responsible for issuing attack instructions and approaching the device to execute commands in the target physical area to carry out penetration work.



(WiFi proximity attack system (basic version) operation status diagram)

The mini version of the system supports disguising itself as a power strip, power adapter, etc. After placing the device in the target physical area, it connects to the WiFi in the target area and establishes a Socks proxy tunnel to achieve close penetration of the target network.



(WiFi proximity attack system (mini version) operation form diagram)

2.1.2 Product functions

WiFi proximity attack system (basic version)

> WiFi password cracking: The system supports scanning and cracking of WiFi (including hidden WiFi and 5G_WiFi) in the target area. Common WEP, WPA, WPA2 and WPS protocols can be cracked. Cracking method: local cloud query, cloud cracking.

> Intranet sniffing: When the approaching device is in the target intranet domain environment, the device actively sniffs the target intranet domain user hash and automatically captures it.

▷ Socks proxy: The system supports setting up the Socks proxy function to map intranet information to the public network for related penetration operations.

>Route cracking: The system supports automatically cracking the login password of the routing device existing in the target intranet to achieve active login and management control of the routing device in the target intranet.

> Port mapping: After the proximity device accesses the target intranet through WiFi, it can map the target host port in the intranet to the Internet to achieve the purpose of accessing the target intranet from the external network.

> Interactive terminal: The system supports the execution of Shell commands and file operations on nearby devices.

> File management: The system supports visual upload and download management of files in nearby devices.

> Remote destruction: When there is a security threat to the device, it supports remote sending of self-destruction commands to completely clear all system data in the device.

WiFi proximity attack system (mini version)

> Network connection: After the device is placed in the target network environment, the connection is set up through its own WiFi signal, and finally connected to the target network.

▸ Socks agent: After the device is connected to the target network, log in to the remote control management system through the PC and open the Socks agent to perform related penetration operations.

2.1.3 Product parameters

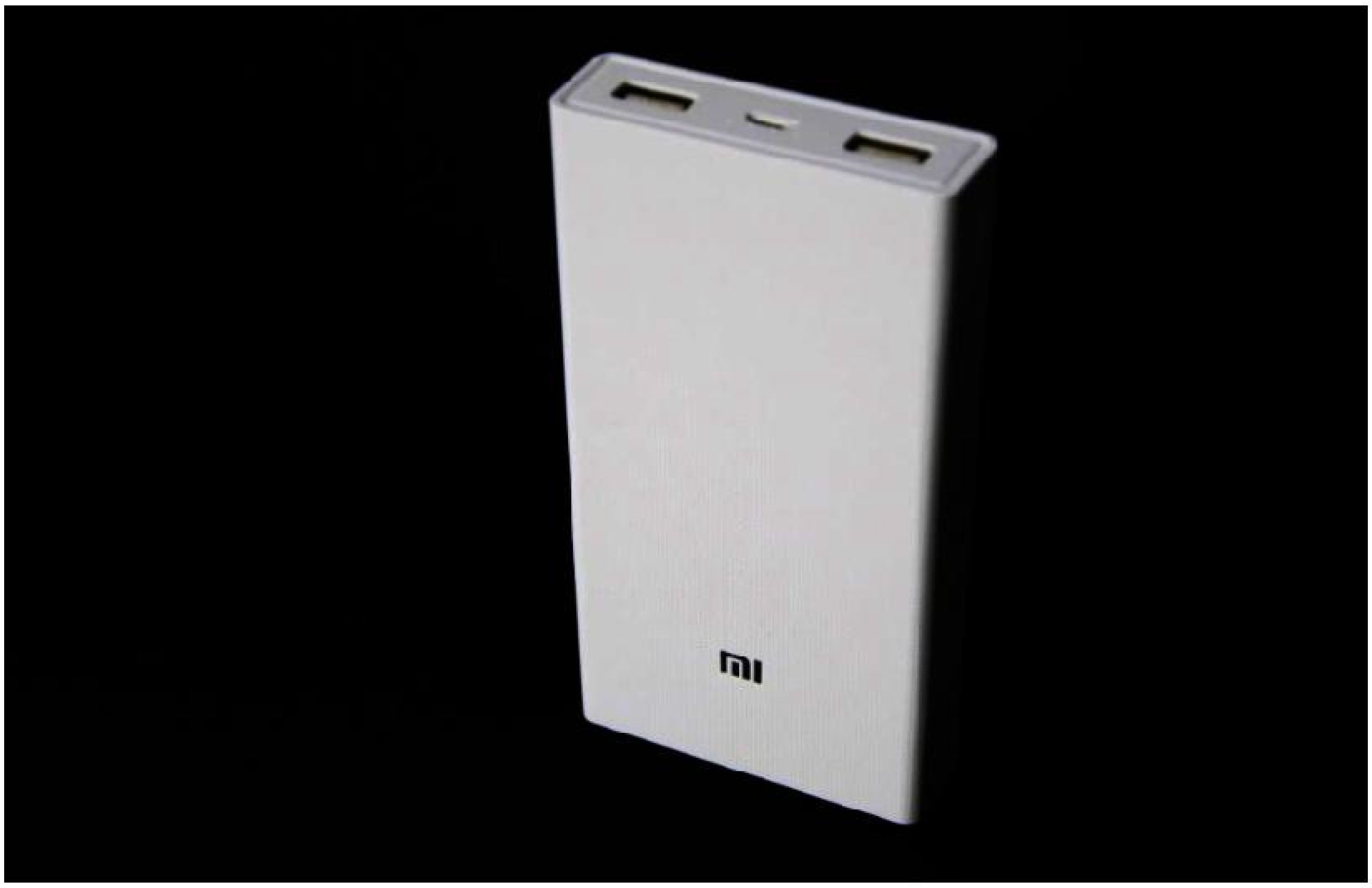
project	WiFi proximity attack system (basic version)	WiFi proximity attack system (mini version)
Architecture	ARM	MIPS
CPU	Main frequency 1.2G, dual core	/
storage	8GB eMMC high-speed flash memory	DDR2 128MB
network	Support all Netcom 4G	Wireless network card 802.11/b/g/n three modes
Built-in battery	10000mA rechargeable lithium battery	none
MCU main frequency	/	580MHz
Flash	/	32MB
WiFi module	Default mode	Support AP/STA and AP/STA mixed mode
Device details	141mm x 73mm x 22mm	41mm x 23mm x 3.5mm

2.1.4 Industry advantages

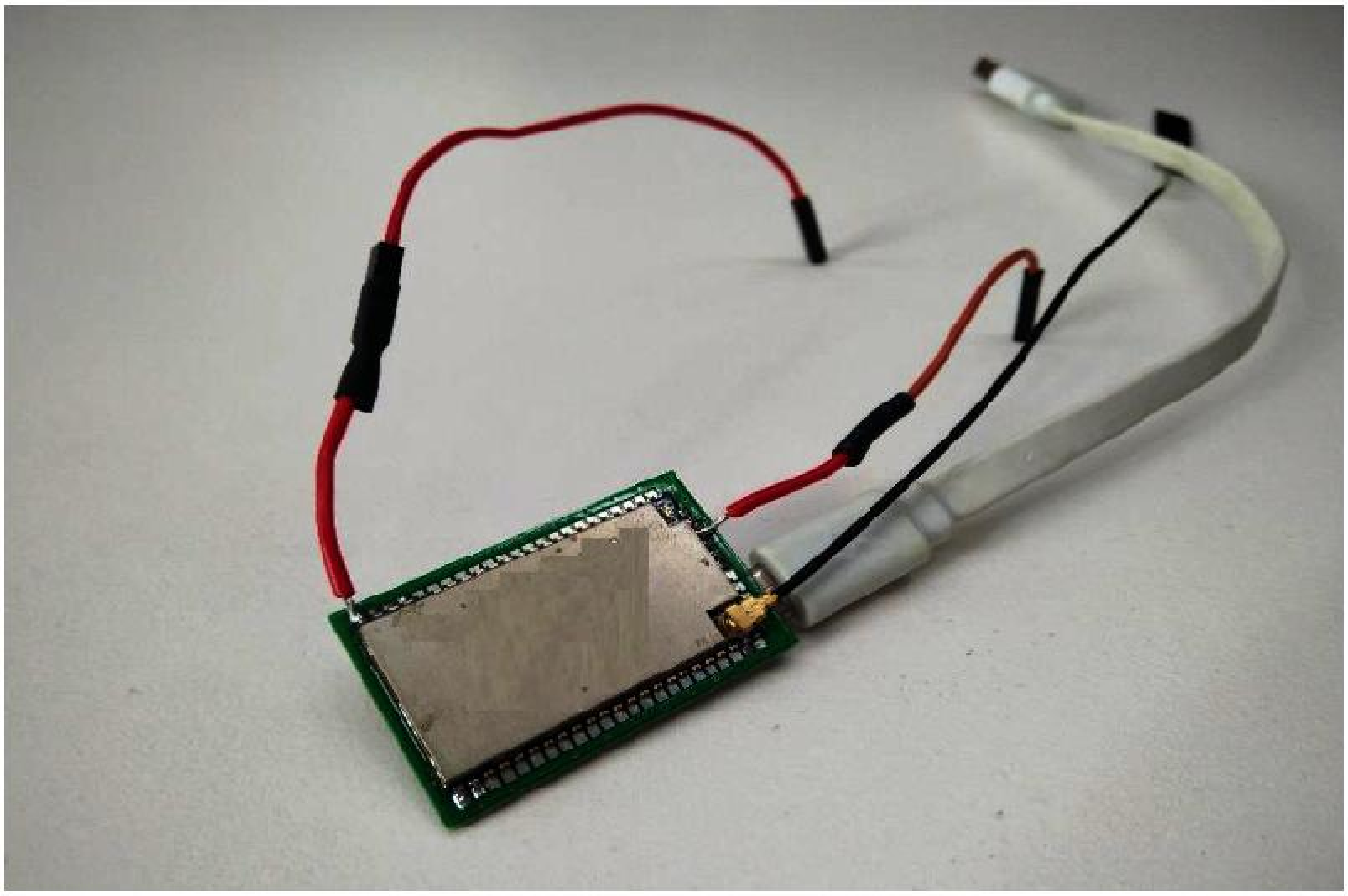
- Strong camouflage——You can choose different versions according to different application scenarios, disguised as Xiaomi power bank or ultra-small circuit board module design, easy to carry and difficult to detect, and can pass security inspections, interrogations and other security measures.
- High ease of use——You only need to carry the device to the designated area and turn on the power. No other operations are required, and the device can be controlled remotely to carry out penetration work.
- High penetration efficiency. The physical proximity of the product hardware is combined with the remote control of the backend network to establish a new intranet penetration channel for penetration work.
- High battery life - The basic version has a built-in large-capacity rechargeable lithium battery, which can last for 8 hours at full load and 20 hours under normal operation, and supports simultaneous operation and charging.

○Easy to operate——The system setting interface is simple and adopts graphical interface. You only need to click the relevant button to complete the operation.

2.1.5 Product pictures



(WiFi proximity attack system (basic version) product picture)

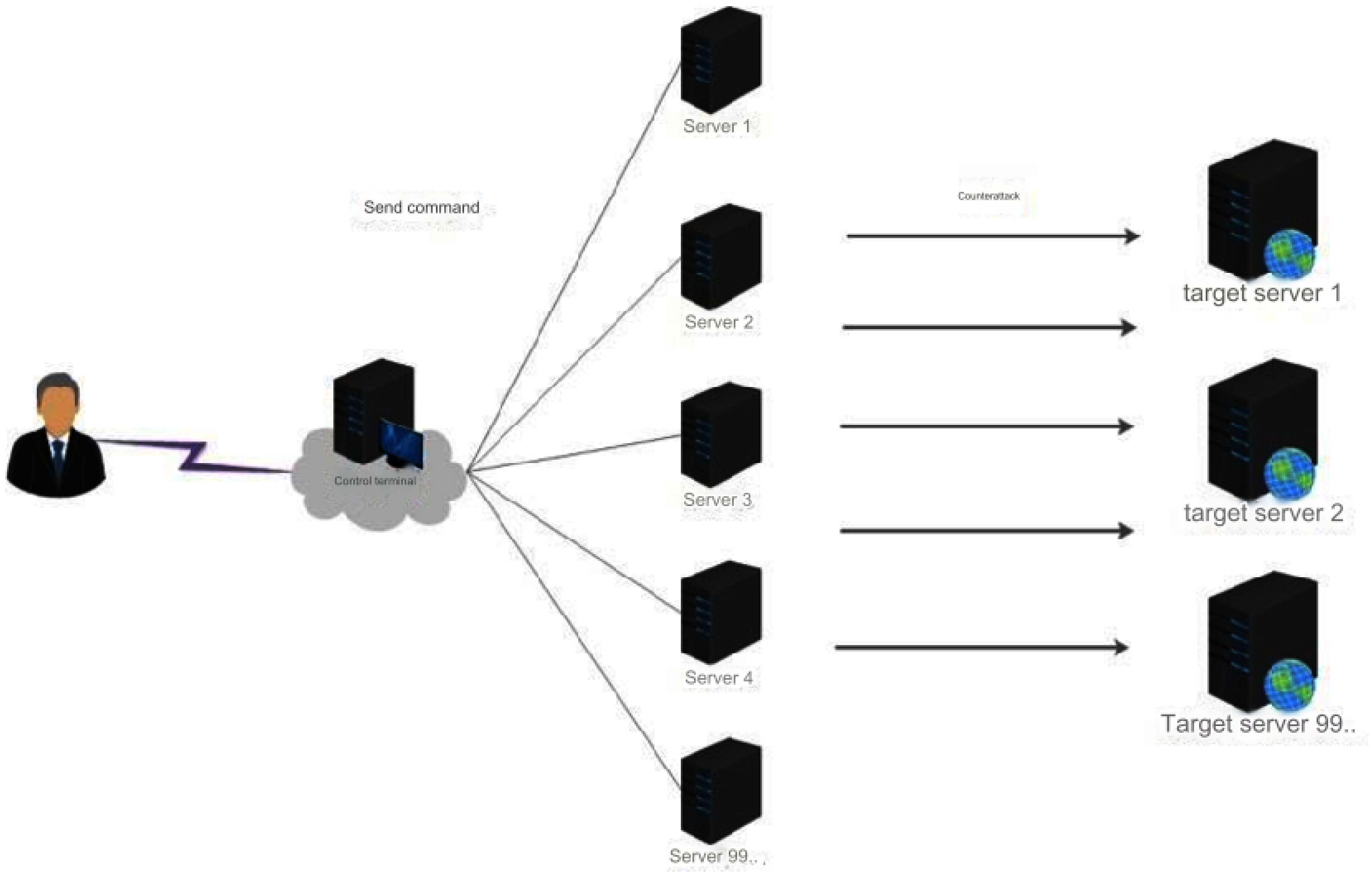


(WiFi proximity attack system (mini version) product picture)

2.2 Network traffic countermeasures system

2.2.1 Product Introduction

The network traffic countermeasure system combines the actual application scenarios of relevant departments and uses active scanning and acquisition technology to obtain global distributed stress test traffic to achieve comprehensive countermeasures against system traffic such as target servers, websites, and enterprise networks. The entire system consists of a counter flow acquisition module and a counter flow control module.



(Network traffic countermeasure system operation form diagram)

The system coexists C/S and B/S architectures, fully absorbing the characteristics of the two architectures. The counter-traffic acquisition module uses active scanning and acquisition technology to acquire global surviving network traffic and conduct comprehensive automated massive vulnerability detection to provide network traffic data for the counter-traffic control module.

The countermeasure flow control module is used to control all nodes and uniformly issue the received countermeasure instructions. It also provides dedicated anonymous links for safe and efficient data communication. During use, the system supports a variety of external interfaces to facilitate users for secondary development.

2.2.2 Product functions

> Counter traffic acquisition: By configuring the counter flow control module, start the counter traffic acquisition module, use asynchronous transmission scanning technology to obtain global surviving network traffic, automatically filter and clean invalid network traffic, and perform vulnerability detection and utilization of effective surviving traffic , and finally achieve the acquisition and control of countermeasures traffic.

> Stress test: supports regular mode (SYN, UDP, TCP, ACK, IGMP, ICMP, DNS), Web mode (Get protocol, mutated CC, unlimited CC, distributed loop CC), breach mode, etc., as well as powerful automatic Definition mode, supports hexadecimal and ASCII code conversion. It supports multi-mode simultaneous stress testing. The unique UDP countermeasure technology, combined with the new kernel technology, sends data packets directly to the target without going through the buffer area.

> Cluster management: supports cluster management of online hosts, assigns designated tasks to online hosts, can perform cluster countermeasures against target IPs, individual target countermeasures, loop through target countermeasures, and automatically loop through to find effective countermeasures packets.

2.2.3 Product parameters

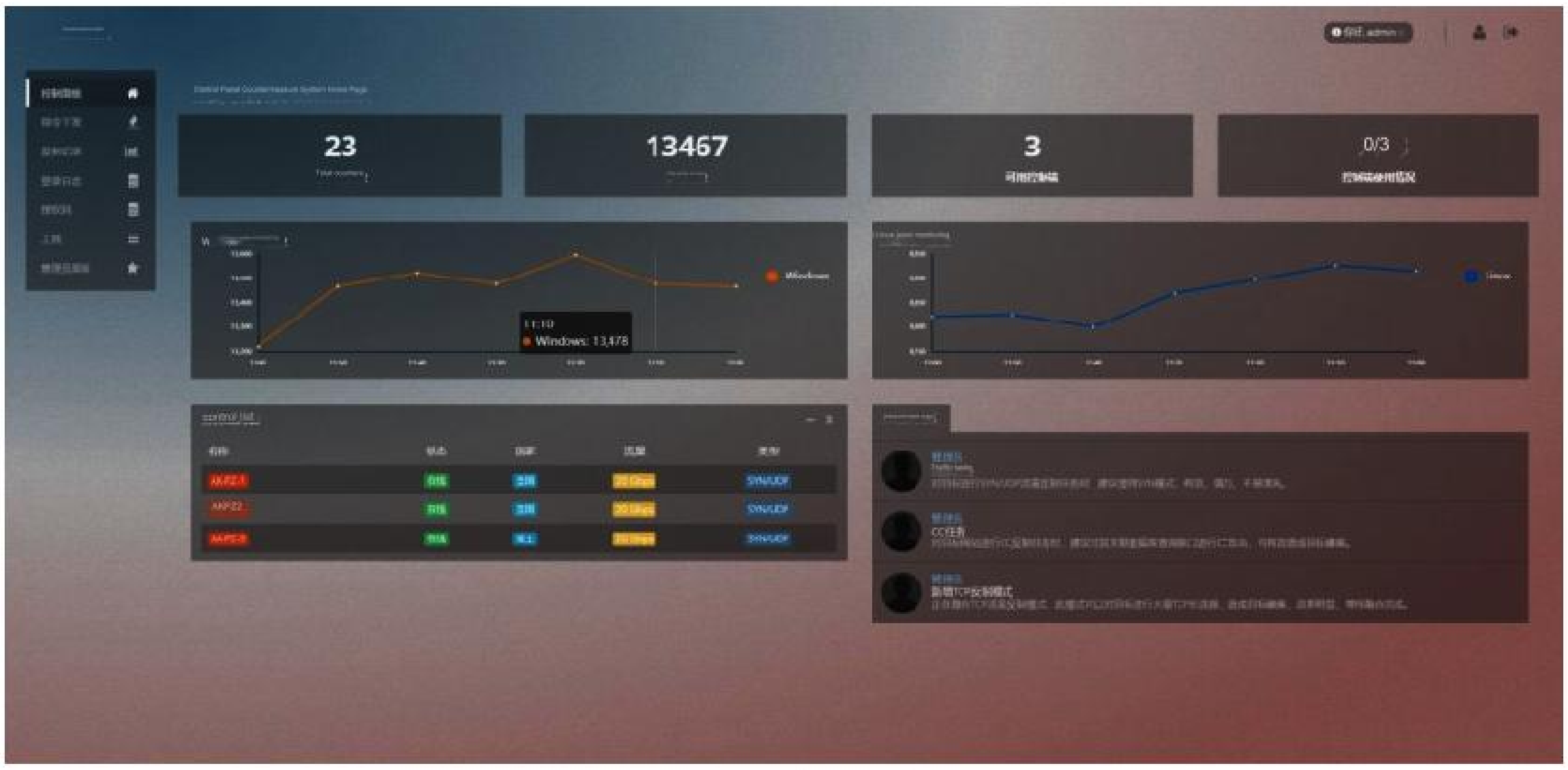
project	parameter
scanning method	asynchronous transfer
Scan thread	Max 1000
Maximum concurrent tasks	20
Vulnerability type	Remote code execution, weak passwords, databases, Web, etc.
Online quantity	30000—60000
Traffic output scale	10G—100G
Client size	29Kb
Communication mode	TCP/HTTP
Countermeasure mode	SYN、UDP、TCP、ACK、IGMP、ICMP、DNS、CC
Online method	IP/domain name
Start mode	system service
Support platform	Windows/Linux/IoT

2.2.4 Industry advantages

- Cross-platform - perfectly compatible with all Windows systems: Windows XP/Vista/7/8/8.1/10; Windows sever 2000/2003/2008/2012/2016. It is compatible with Linux/CentOS/Ubuntu/AIX/Solaris/HP-UX and other systems and mainstream IoT device systems.
- High flexibility——The system supports intelligent countermeasures function, which can automatically choose whether to carry out countermeasures according to the survival status of the countermeasure target.

- Simple operation and configuration——The system adopts a graphical design interface, which is convenient and quick to deploy. It adopts one-click configuration operation to quickly achieve the acquisition and control of countermeasure traffic.
- The system is stable and reliable——The system adopts the latest network traffic acquisition and control technology, comprehensively considers the stability, efficiency and reliability in various application scenarios to ensure the stable operation of the system in an all-round way.

2.2.5 Product pictures

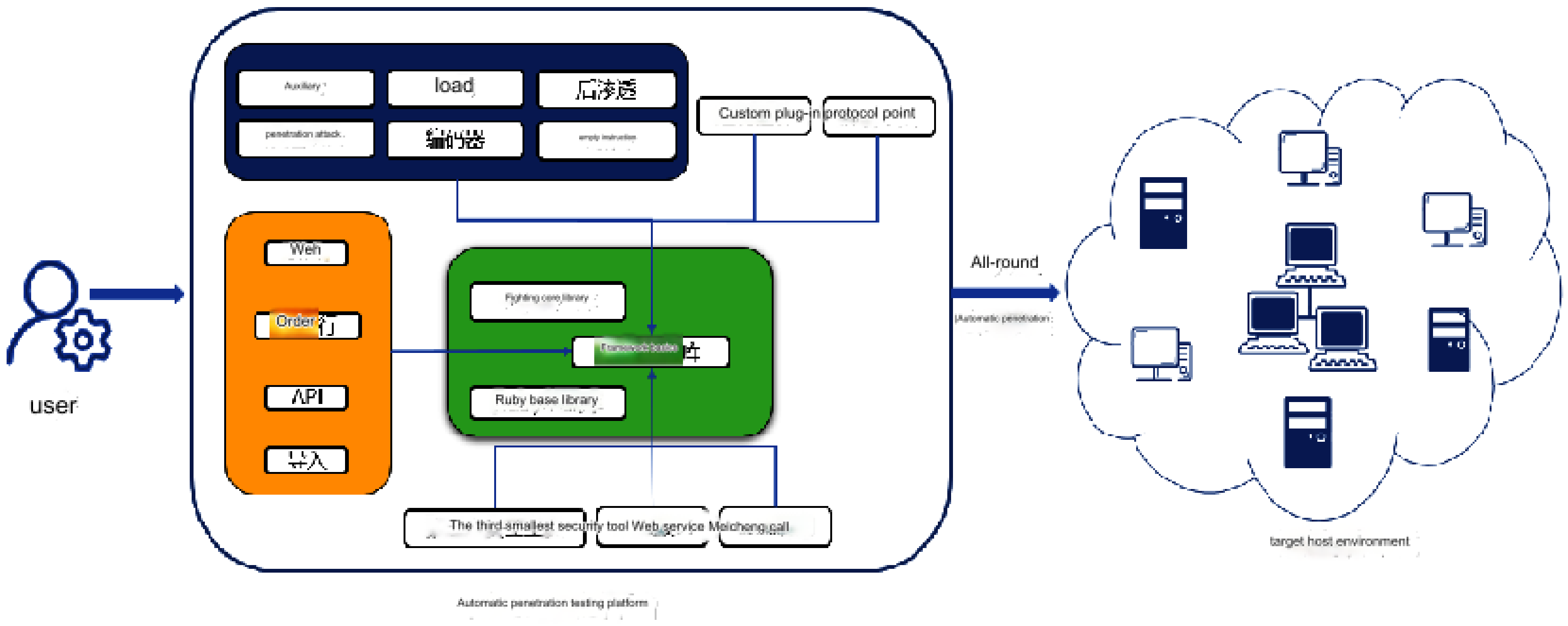


(Network traffic countermeasure system interface diagram)

2.3 Automated penetration testing platform

2.3.1 Product Introduction

The automated penetration testing platform is a platform that integrates hundreds of vulnerability templates and penetration testing methods to support automated penetration testing of various network devices and hosts. Attack the real production environment through a variety of testing methods built into the platform to achieve information detection, vulnerability verification, vulnerability exploitation, penetration attacks and report generation on the network and equipment under test, improving the efficiency, convenience, completeness and accuracy of penetration testing sex.



(Automated penetration testing platform operation form diagram)

2.3.2 Product functions

- Automated penetration: Through a series of processes such as vulnerability scanning, vulnerability exploitation, and permission acquisition, the target's open ports and services are discovered. Based on the detected information, the system exploits vulnerabilities to further obtain target permissions. The specific content is as follows:

a) Vulnerability scanning

1) Vulnerability quick scan: Conduct quick scan tests on various targets such as Windows hosts, Linux hosts, Web sites, network devices, etc. to determine host online status, open port status, operating system version and other information, and generate a report on the results.

2) Detailed vulnerability scanning: The system has tens of thousands of built-in detection templates and vulnerabilities, supports Web vulnerability scanning, operating system vulnerability scanning, weak password detection and other functions, proactively analyzes all weaknesses, technical flaws or vulnerabilities of the system under test, and reports the results Generated reports include: host information, vulnerability assessment, vulnerability details, vulnerability exploitation, service list, port information, database information, file directory information, scanning history, etc.

b) Exploiting vulnerabilities

1) Vulnerability verification: According to the vulnerability scanning results, vulnerability exploitation modules with different risks can be customized and selected to perform penetration attacks on the target vulnerabilities.

2) Import of scan results: The platform supports the import of scan results and vulnerability verification from a variety of third-party security scanning tools, automatically identifies and imports reports, and selects the imported host and corresponding vulnerabilities to be penetrated and verified in the system. After confirming that the vulnerability is real, it can be attacked. . Support includes: NSFOCUS Aurora, Venus Sky Mirror, AppScan, NeXpose, Acunetix, Core Impact, Nessus,

NetSparker, Nmap, etc.

c) Permission acquisition: After the vulnerability is successfully exploited, the system supports the selection of a series of execution codes and script programs written according to the vulnerability exploitation method based on the penetration results to achieve the acquisition of target permissions.

> APT attack

a) Email phishing: The platform supports designated email sending servers, uses Web page components to clone and forge Web sites, establishes email content templates for the forged sites, induces targets to submit sensitive information on the forged Web sites, and ultimately collects the target's sensitive information for For further attack purposes.

b) Browser attack: The platform supports the establishment of a site that automatically detects browsers and exploits vulnerabilities through Web page components. The target is induced to browse the specified site. After the browser vulnerability is successfully exploited, a connection session is automatically established.

c) File vulnerability attack: The platform supports file vulnerabilities such as Office, PDF, pictures, etc., and generates files with attack payloads. The target is tricked into typing or browsing files, and a connection session is automatically established after the vulnerability is successfully exploited.

> Web attack: The platform supports crawling the specified range of web pages for the input URL, and using the Web test module to test the page, including: automatic testing of the latest top ten Web security vulnerabilities listed by OWASP, misconfiguration of the Web server, cross-border Website script attack vulnerabilities, local file inclusion and remote file inclusion, SQL injection vulnerabilities, file second pass vulnerabilities, remote code execution vulnerabilities or remote command execution vulnerabilities.

> Other functions

a) Load generator

1) Classic payload: The platform supports generating a variety of attack payloads for penetration testing. The generated payload supports various operating systems and commonly used web server-side languages, including: Linux, Unix, AIX, BSD, R, Windows, OSX, Netware, iOS, Android, Firefox, Java, Python, Ruby, NodeJS, etc.

2) Dynamic payload: The system supports the generation of a variety of dynamically encoded attack payloads targeting the Windows platform to evade detection by anti-virus software.

b) Brute force cracking: The system supports brute force cracking of weak passwords and uses dictionaries to detect weak passwords in the network. You can choose the credentials, default dictionary or imported dictionary in this project. Supports cracking various types of

Common protocols, databases and service types, including: FTP, HTTP, HTTPS, SMB, SNMP, MSSQL, MySQL, DB2, Postgres, POP3, SSH, SSH PUBKEY, Telent, NVC, WinRM c

c) Credential reuse: The system supports using passwords or hash value credentials obtained during penetration testing assessments to test other hosts on the network, effectively testing and discovering possible horizontal expansion paths for users.

d) Replay attack: For a successful penetration attack, after the session established with the target is suspended or disconnected, there is no need to re-carry out complex attack operations. You can choose to replay the attack directly and re-infiltrate based on the previous attack parameters. and establish a session.

e) Springboard attack: For advanced usage scenarios, after successfully penetrating a host, the penetrated host can be used as a springboard to further attack other targets.

> System management

a) Report generation: The platform supports report generation in three file formats: HTML, PDF, and World. You can customize reports or use a variety of built-in report templates. Report templates include: audit, information collection, vulnerable hosts, credentials, services, and social engineering activities. , Web application testing, etc.

b) System settings: Supports platform data backup, task monitoring, user account creation, role permission settings, system authorization management, setting periodic tasks, regular automated penetration inspections and other operations.

2.3.3 Product parameters

project	parameter	Standard Edition	Professional version
Quick scan takes time	Average time spent on 1-5 hosts	30 minutes	30 minutes
Default concurrent scan	Default number of hosts scanned simultaneously	5	5
Number of vulnerability libraries	100,000+	support	support
Number of vulnerability check items	300,000+	support	support
Maximum concurrent scans	Maximum number of hosts scanned simultaneously	10	10
Total number of modules	Including utilization, assistance, post-infiltration and other modules	1000+	1000+
Number of modules utilized	Only use the number of modules	1700+	1700+
IP number authorization	Whether to limit the total number of target IPs	unlimited	unlimited
Web interface	Operate via browser interface	support	support
Command line operation	Operation via terminal command line	support	support
Support IPv6	Support IPv6 network scanning	support	support
independent property rights	Code is completely autonomous	support	support
Exploit coverage	Including operating systems, network equipment, databases, middleware, system software, etc.	support	support

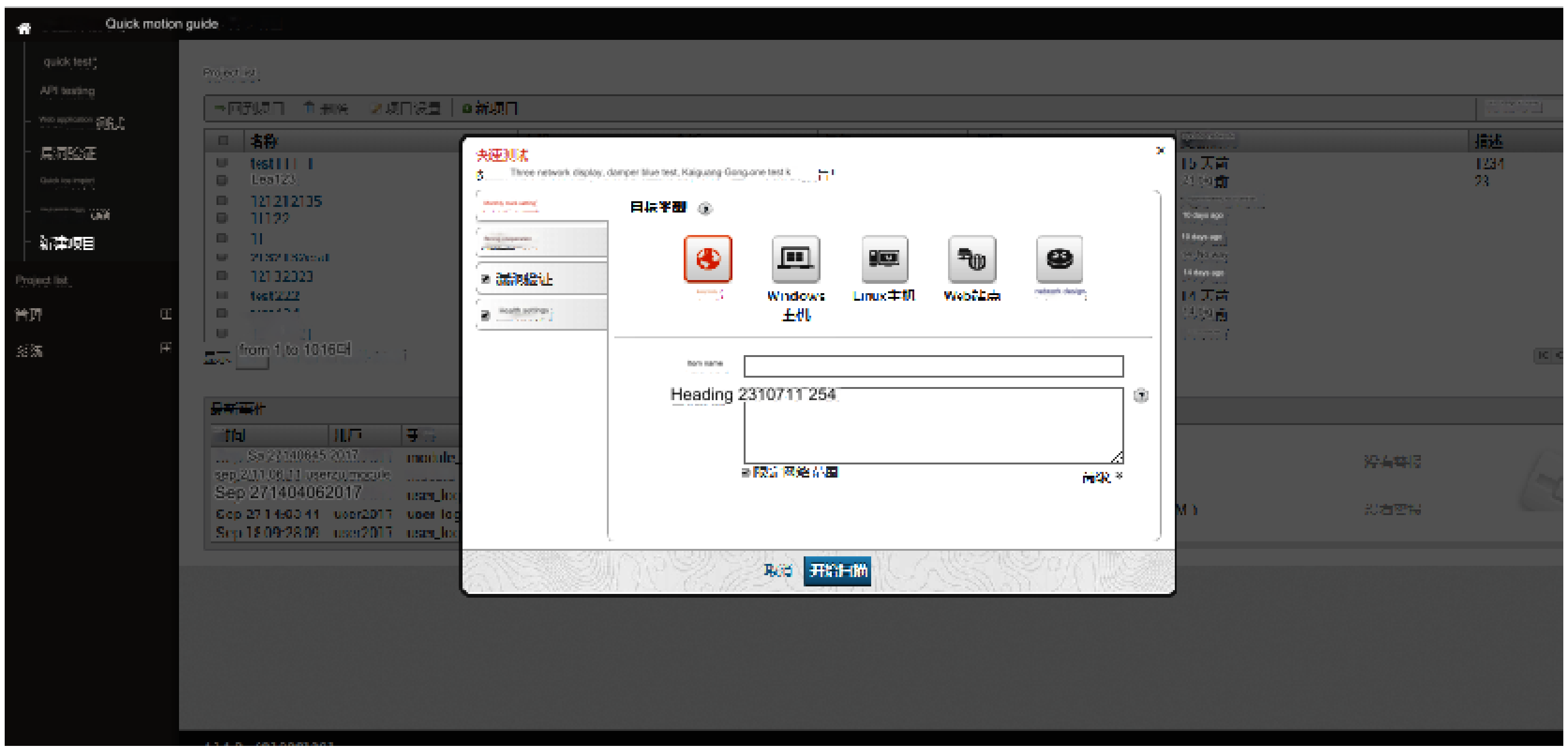
Password Brushing Support Protocol	Protocols: AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, SSH PUBKEY、Telnet、VNC、WinRM	support	support
Sub-project management	Supports project-based management of penetration testing targets.	support	support
quick guide	Quick guide for common penetration testing operations.	support	support
Web audit	Scan and audit web applications	support	support
External report import	Import report results scanned by third-party applications	support	support
Vulnerability verification	Conduct penetration testing and verification of scanned vulnerabilities (reports of mainstream leaks, such as NSFOCUS and Qiming)	support	support
Credential reuse	Test other hosts with the found credentials	support	support
evidence collection	Collect evidence of successfully exploited target vulnerabilities	support	support
Post penetration module	Modules available for post-penetration operations	support	support
Automatic post penetration	After successful exploitation, customized post-infiltration can be automatically executed. module	support	support
Session persistence	The session after successful utilization can be persisted	support	support
social engineering attack	Assist social engineering testing to test people 男Safety awareness	support	support
IDS/IPS bypass	Support configuration parameters to try to bypass IDS/IPS	support	support
Avoid anti-virus software	Supports a certain degree of anti-kill function when infiltrating	support	support
Set in the Netherlands	Supports generating specifically configured attack payloads	support	support
Agency Springboard	Supports the use of proxy springboards for intranet penetration	support	support
VPN Springboard	Supports the use of VPN springboards for intranet penetration	support	support
replay attack	Supports replay of previously successful attacks	support	support
Generate report	Supports report generation for security testing assessments	support	support
report format	HTML\PDF\WORD	support	support
Number of report templates	Number of different report templates	support	support
Customized reports	Supports customization of report content Number	support	support
support the maximum number of users	of users supported by the web interface	1	3
Scheduled Tasks	Supports advanced automated scheduled tasks	support	support
Vulnerability assessment support scope	Operating systems (Windows, Linux, UNIX, OS, etc.), databases (SQL Server, DB2, Oracle, MySQL, etc.), Web applications, middleware, network equipment (routing, switching, firewalls, etc.)	support	support
Black box vulnerability assessment	Assess vulnerabilities through network remote fingerprinting	support	support
White box vulnerability assessment	Login scan using login credentials	support	support
Scan policy template	Built-in more than 8 scanning policy templates for different vulnerability assessment requirements	support	support
Custom scan strategy	Scanning strategy templates can be customized and configured	support	support

Exploitable vulnerability information	Prompt vulnerabilities that have publicly exploited methods, provide source information of relevant vulnerability exploits, etc.	support	support
Vulnerability judgment basis	The scanned vulnerabilities can be viewed based on the	support	support
Accurate risk scoring	judgment. In addition to the CVSS standard vulnerability score, a more accurate risk score is provided based on asset importance, vulnerability exposure, threat level, etc.	support	support
Virtualization platform scan	Supports scanning of mainstream virtualization platforms such as VMware/KVM, etc.	support	support
Weak password scanning	Supports weak password scanning for common protocols	support	support
baseline scan	CIS, customized baseline scan guide	support	support
Enhanced web scanning capabilities	Able to detect Web applications and Web Services applications based on Javascript, Ajax and Flash (including SOAP 1.2, Json, WSDL, XML), and detection cases can cover all OWASP Top 10 threats	not support	support
API interface	Provide API interface for external applications to adjust the month	not support	support

2.3.4 Industry advantages

- Automation————The entire penetration attack platform consists of six parts: intelligence collection, threat modeling, vulnerability analysis, penetration attack utilization, post-penetration testing, and reporting. It provides automated support for the entire penetration testing process according to different penetration environments.
- The professional-level vulnerability library system has built-in Metasploit commercial-level professional version vulnerability exploitation platform, which integrates thousands of operating systems, application software vulnerabilities, and hundreds of shellcodes, and is constantly updated to fully meet the needs of in-depth vulnerability scanning.
- Flexible custom scanning——Supports customizing the start time of website scanning to avoid website business peaks, or setting periodic scanning tasks according to the needs of the business online process.
- Flexible expansion—the platform supports local deployment and distributed deployment to cope with emergencies during the penetration process, and intelligently schedules the penetration process without interruption, improving the reliability, availability and scalability of the platform.

2.3.5 Product pictures



(Automated penetration testing platform interface diagram)

2.4 WiFi terminal positioning countermeasures equipment

2.4.1 Product Introduction

WiFi terminal positioning countermeasure equipment is a product that uses the directionality of directional antennas to determine the positioning of WiFi devices based on signal strength for WiFi signals.

2.4.2 Product functions

> Scanning WiFi devices: Supports scanning the wireless signals of surrounding APs and terminals, performing operations such as pinning them, filtering conditions, and creating snapshots of scanned information.

> Positioning WiFi devices: Supports wireless device positioning, real-time alarms and target discovery based on signal changes in MAC addresses, voice broadcast of the current positioning signal value and real-time display of the signal change direction. The positioning accuracy is less than 1 meter.

> Counter WiFi devices: Supports active discovery of APs and terminals, tracks their signals, blocks them, and disconnects them from the network.

2.4.3 Product parameters

hardware module	Parameter item	Parameter value
radar equipment	Battery	1000mAh, 8 hours battery life
	CPU	Quad-core 1.2GHz 64-bit
	running memory	1GB
	size	240*190*40mm
	Number of WIFI modules	4
	disk	8GB
	Positioning distance	>100m
	positioning accuracy	<1m
Control your phone	Battery	3000mAh
	running memory	1GB
	Body memory	8GB
	size	5.5 inches

2.4.4 Industry advantages

- Long coverage distance——Using special power amplifier directional antenna and WIFI module to provide high-power wireless signal and long coverage distance.
- Accurate positioning——Use the directionality of the antenna to determine the direction of the WiFi device, and then determine the distance based on the signal strength to achieve accurate positioning.
- Strong concealment————The device is portable and lightweight, controlled by Caiyue's mobile phone, and has strong concealment.

2.4.5 Product pictures

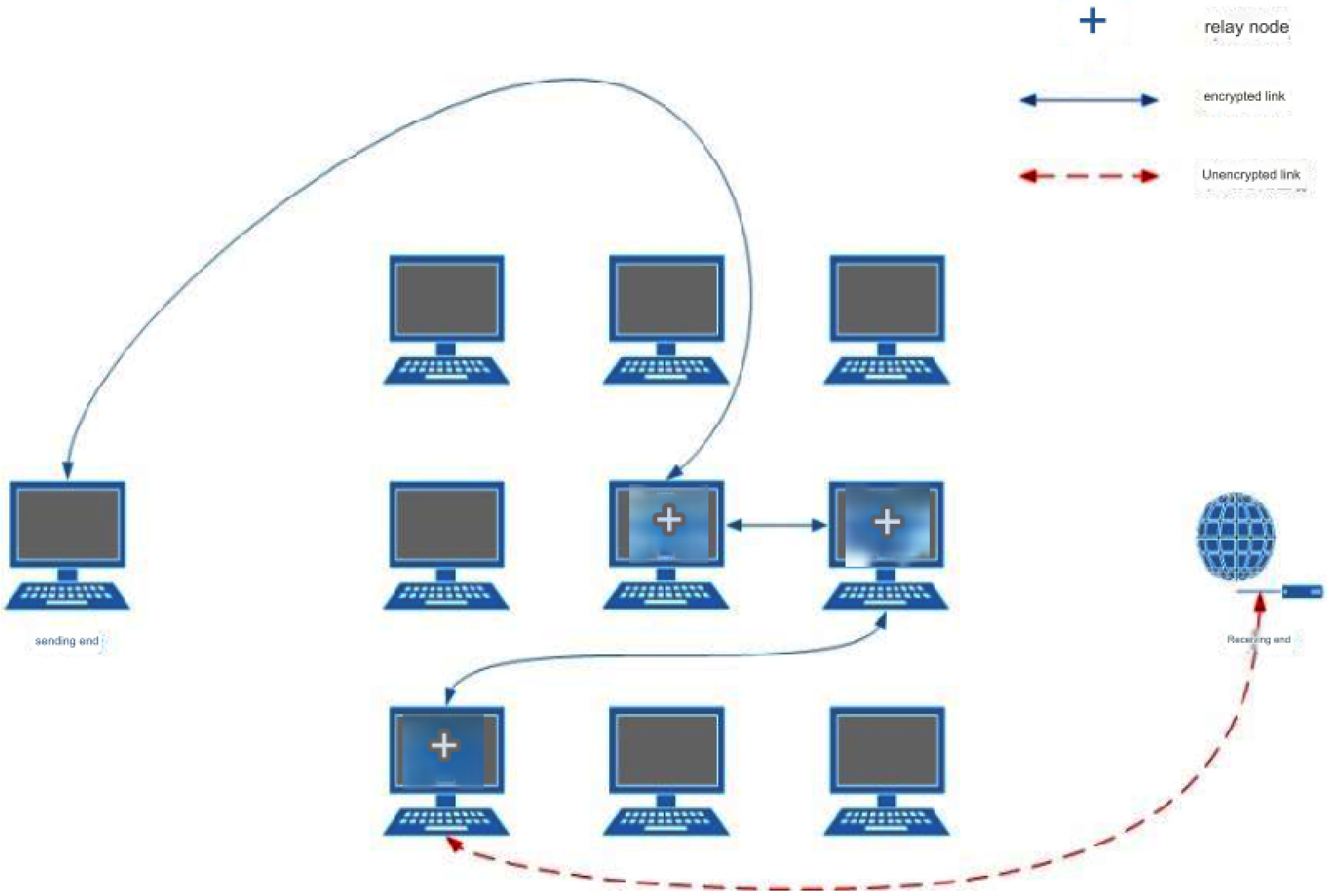
(WiFi terminal positioning and countermeasures equipment product appearance picture)

Three security cover categories

3.1 Anonymous anti-tracing wall

3.1.1 Product Introduction

Anonymous anti-tracing wall is an anonymous communication network product developed by Anxun Information. It is used for overseas network special investigation work. It hides the user's real IP address, physical address, and interaction through strong link encryption, multi-node jumps, and random changes in exits. A product that enables anonymous surfing of sensitive information such as content. The system can prevent sensitive information from being tracked and eliminate security risks.



(Anonymous flood wall operation pattern diagram)

3.1.2 Product functions

- Anonymous Internet access: The system is connected to the Internet, and after passing through several relay servers, it hides sensitive information such as real exits, real IP addresses, and physical addresses to achieve anonymous secondary network functions. Prevent sensitive information from being tracked.

- Port mapping: Supports mapping the corresponding service ports of the intranet terminal to the corresponding peripheral server to achieve the purpose of the external network accessing intranet-related applications. It can be used in scenarios where it is necessary to accept data returned from the external network.

3.1.3 Product parameters

parameter	Anonymous anti-tracing wall
length, width and height	28.2*16.1*4.3(cm)
CPU	Dual core 800MHz
Memory	512MB DDR3
interface	4 10/100/1000M adaptive LAN ports 1 10/100/1000M adaptive WAN port 4 LAN port lights 1 WAN port light 1 POWER light 1 SYS light 1 ERROR light 1 power input port
4G Internet access	support
Internet speed	The maximum download speed can reach 700KB/S
relay node	Unlimited nodes, three jumps
access device	Mobile phones, tablets, desktop computers, laptops

3.1.4 Industry advantages

- Multiple networking methods——Support PPPOE connection method for Internet access, network cable connection to upper-level router for Internet access (DHCP or static IP), 4G dial-up and other networking methods.
- Plug and play——Combined with the actual network environment, users can achieve scientific Internet access or anonymous secondary network through simple configuration of the anonymous network system.
- High egress bandwidth——10M/100M egress bandwidth fully meets bandwidth requirements.
- High concealment——The system deploys hundreds of mouth relay nodes, adopts a random selection strategy, and can combine hundreds of thousands of communication paths, and the exit node will automatically update the selection every 5-10 minutes, effectively preventing traffic from being analyzed track.
- Strong security——All-communication data of the system are transmitted using unique encryption technology to effectively avoid being monitored.
- High ease of use——You can surf the Internet anonymously by simply using the terminal for simple configuration.

3.1.5 Product pictures

(Anonymous flood wall product physical picture)

Four other product categories

4.1 Domestic public opinion tracking system

4.1.1 Product Introduction

The Domestic Public Opinion Investigation System is a dedicated confidential application system that serves actual operations and provides real-time query of netizen registration information on multiple mainstream interactive network platforms such as Baidu, Sina, Tianya, etc.

4.1.2 Product functions

> Sina Weibo information query: Weibo link or nickname query mobile phone, mobile phone or email query Weibo ID, Weibo historical login IP, Weibo picture traceability.

1) Query mobile phone by Weibo link or nickname: Through Sina Weibo URL or nickname, you can associate the registered mobile phone number and email address of its Sina Weibo user.

2) Query Weibo ID via mobile phone or email: You can associate its Sina Weibo nickname or ID with your mobile phone or email number.

3) Weibo historical login IP: Through the Sina Weibo nickname, the historical login IP, login time and location of the account can be associated.

4) Weibo picture traceability: Through the Sina picture URL, you can trace the Sina Weibo nickname and ID, and further associate the mobile phone number bound to the account.

> Baidu information query: Nickname query mobile phone, mobile phone or email query account, query anonymous account, Baidu network disk landing.

1) Nickname query mobile phone: Through Baidu user account or nickname, you can associate the bound mobile phone number of its Baidu user.

2) Account query via mobile phone or email: You can associate your Baidu user account or nickname through your mobile phone or email account.

3) Query the unknown anonymous account: Through the Baidu Know anonymous link, you can associate its Baidu user nickname and further associate its bound mobile phone number.

4) Baidu Netdisk implementation: Sharing links through Baidu Netdisk can be associated with their Baidu user nicknames and further associated with their bound mobile phone numbers.

> Tianya Forum information query: Through the Tianya monthly household ID, you can associate the bound mobile phone number of its Tianya user, or associate its Tianya ID according to the mobile phone number.

> WeChat information query: Add friend QR code to analyze WeChat ID, WeChat payment code to analyze WeChat ID, and query WeChat by mobile phone or QQ number.

1) Use the friend QR code to analyze the WeChat ID; associate the friend's QR code with their WeChat ID.

2) WeChat payment code analysis WeChat ID: associate its WeChat ID through the WeChat payment QR code.

3) Query WeChat by mobile phone or QQ number: associate the mobile phone or QQ number with its bound WeChat ID.

▸ Mala community information query: Through the Mala community user tid, you can associate its bound mobile phone number.

> QQ tribe information query: Submit the link URL of the QQ tribe article to associate with its QQ tribe information.

> Operator real-name reference: supports fuzzy name query for China Unicom mobile phone number.

> Probe functions: IP positioning, expression probe, link probe:

1) IP positioning: Enter the IP and associate its IP positioning address.

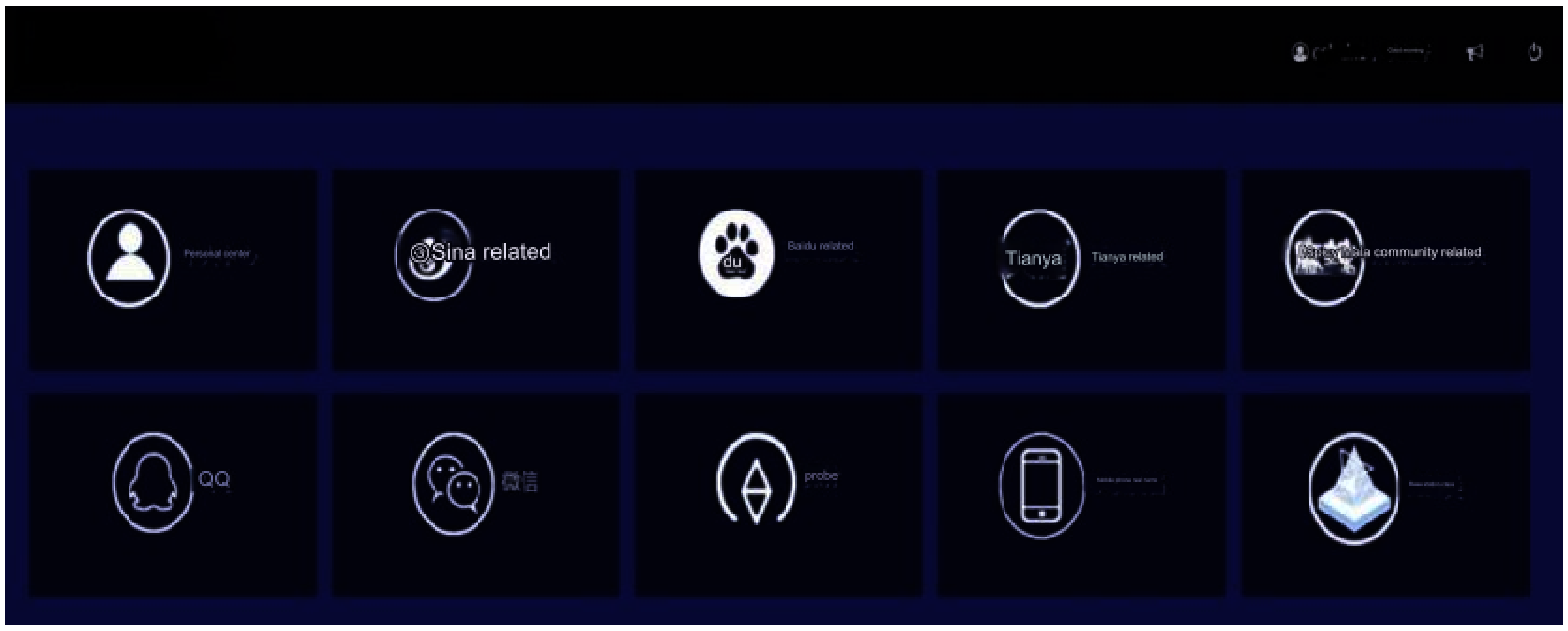
2) Emoticon probe: Send an emoticon picture link to the target in the interactive forum. After the target is opened, the target's IP, port, time, browser version and other information are obtained.

3) Link probe: Add a hyperlink to the article. After the target is clicked, the target's IP, port, time, browser version and other information are obtained.

4.1.3 Industry advantages

- High ease of use——The interface is simple and easy to operate. You can obtain query information by inputting user information as required.
- Quick query——Quickly obtain the returned information through real-time online query through the Internet.
- Rich content——supports querying related information of multiple mainstream platforms such as Baidu, Sina, Tianya, Mala Community, etc.
- High security——Multi-layer encryption of the link is used during the query process to ensure the security of data acquisition.

4.1.4 Product pictures



(Interface diagram of domestic public opinion investigation system)

4.2 Falcon Anti-Gambling Platform

4.2.1 Product Introduction

The Falcon Anti-Gambling Platform is a product professionally designed for relevant departments with the goal of combating online gambling crimes. Provides mining, analysis, and judgment of online gambling data. Based on the data information provided by Yiyi, relevant departments can quickly identify suspected targets based on data characteristics and detailed information. With the support of the platform's online gambling data, they can carry out in-depth online gambling crime investigation tasks to Achieve an overall crackdown on online gambling organizations.

4.2.2 Product functions

> Data query: Users can search for relevant identity information according to their needs. Identity information includes account name, attributes, password, name, screen name, mobile phone number, mobile phone location, email address, login IP, login IP location, address, superior agent, etc. Various types of information, for suspicious identities, you can click the operation button to view detailed information and file a case.

> Case management: The platform supports case investigation and analysis based on the queried basic information of gambling-related users, and conducts correlation analysis based on the data information of the target account to grasp the target's superior-subordinate relationship network map, offline registration time distribution trend, and bank card case value Proportion, regional distribution of offline users, proportion of good cases of offline users and other information, and supports the editing and deletion functions of cases to supplement and improve the account information on file.

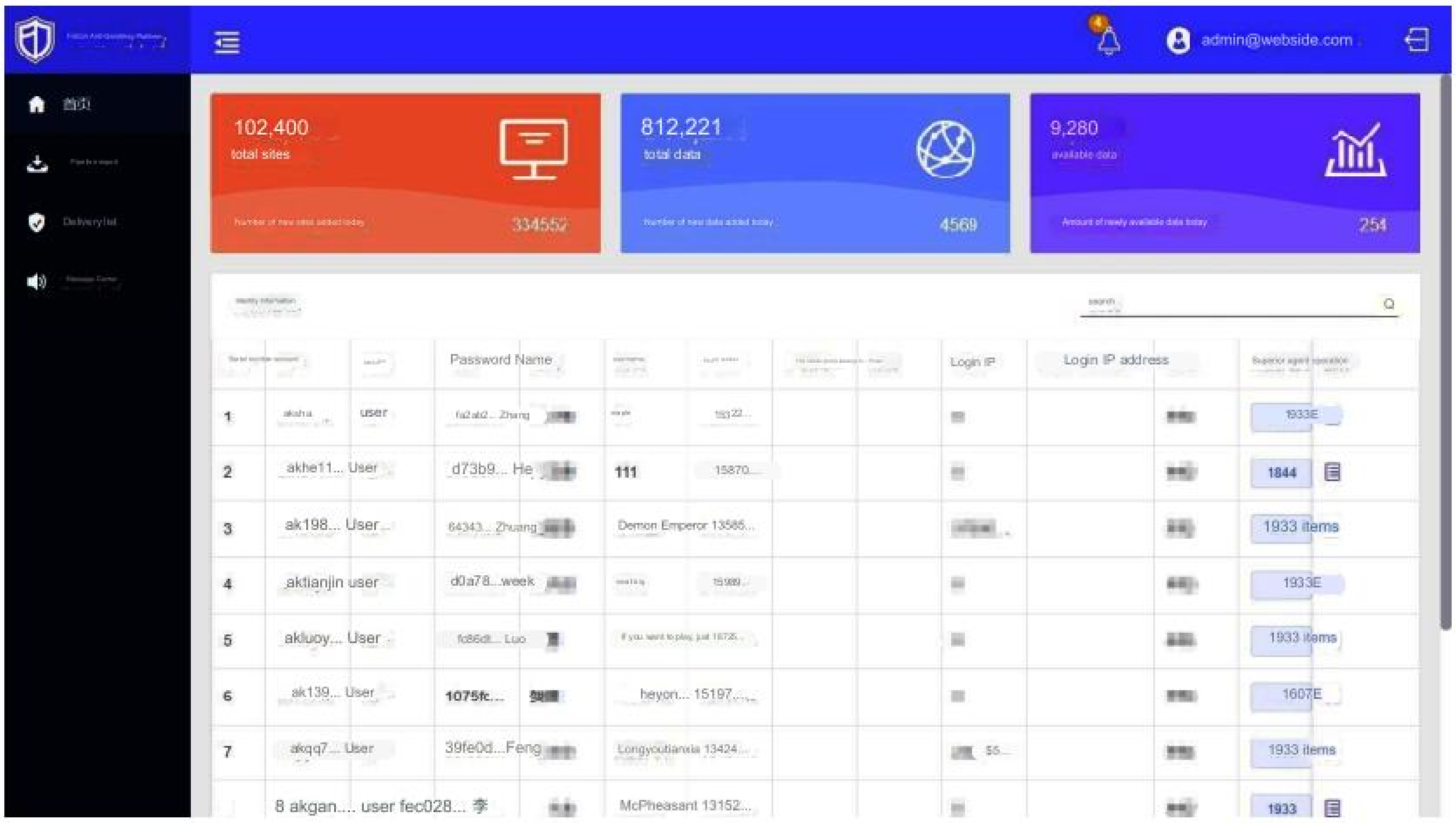
4.2.3 Industry advantages

- Comprehensive and reliable data————The platform provides comprehensive gambling-related user data, provides law enforcement with a large amount of gambling-related personnel account data information, and regularly updates the platform data to ensure the accuracy and effectiveness of the platform's gambling-related data. and reliability.

- Fits the business scenario——The platform is designed based on the business process of gambling-related cases. Through the platform, users can discover suspicious accounts, file investigations, comprehensive analysis and traceability, and finally solve the case, providing a complete business process and case detection ideas. .

- The platform is stable and reliable————The platform is designed based on SaaS services. The data updates and maintenance of the platform are all managed and maintained by professionals to ensure that the entire platform can operate stably 7*24 hours a day and provide users with timely updates. After-sales support service.

4.2.4 Product pictures



102,400
total sites
Number of new sites added today 334552

812,221
total data
Number of new data added today 4569

9,280
available data
Amount of newly available data today 254

Serial number account			Password Name				Login IP	Login IP address	Superior agent operation
1	aksha	user	fa2ab2... Zhang [redacted]	[illegible]	19322...		[redacted]	[redacted]	1933E
2	akhe11...	User	d73b9... He [redacted]	111	15870...		[redacted]	[redacted]	1844
3	ak198...	User	64343... Zhuang [redacted]	Demon Emperor 13565...			[redacted]	[redacted]	1933 items
4	aktianjin	user	d0a78...week [redacted]	[illegible]	15989...		[redacted]	[redacted]	1933E
5	akluoy...	User	fc86df... Luo [redacted]	If you want to play, just 16735...			[redacted]	[redacted]	1933 items
6	ak139...	User	1075fc... [redacted]	heyon... 15197...			[redacted]	[redacted]	1607E
7	akqq7...	User	39fe0d...Feng [redacted]	Longyoutianxia 13424...			[redacted] 55...	[redacted]	1933 items
8	akgan....	user	fec028... 李 [redacted]	McPheasant 13152...			[redacted]	[redacted]	1933

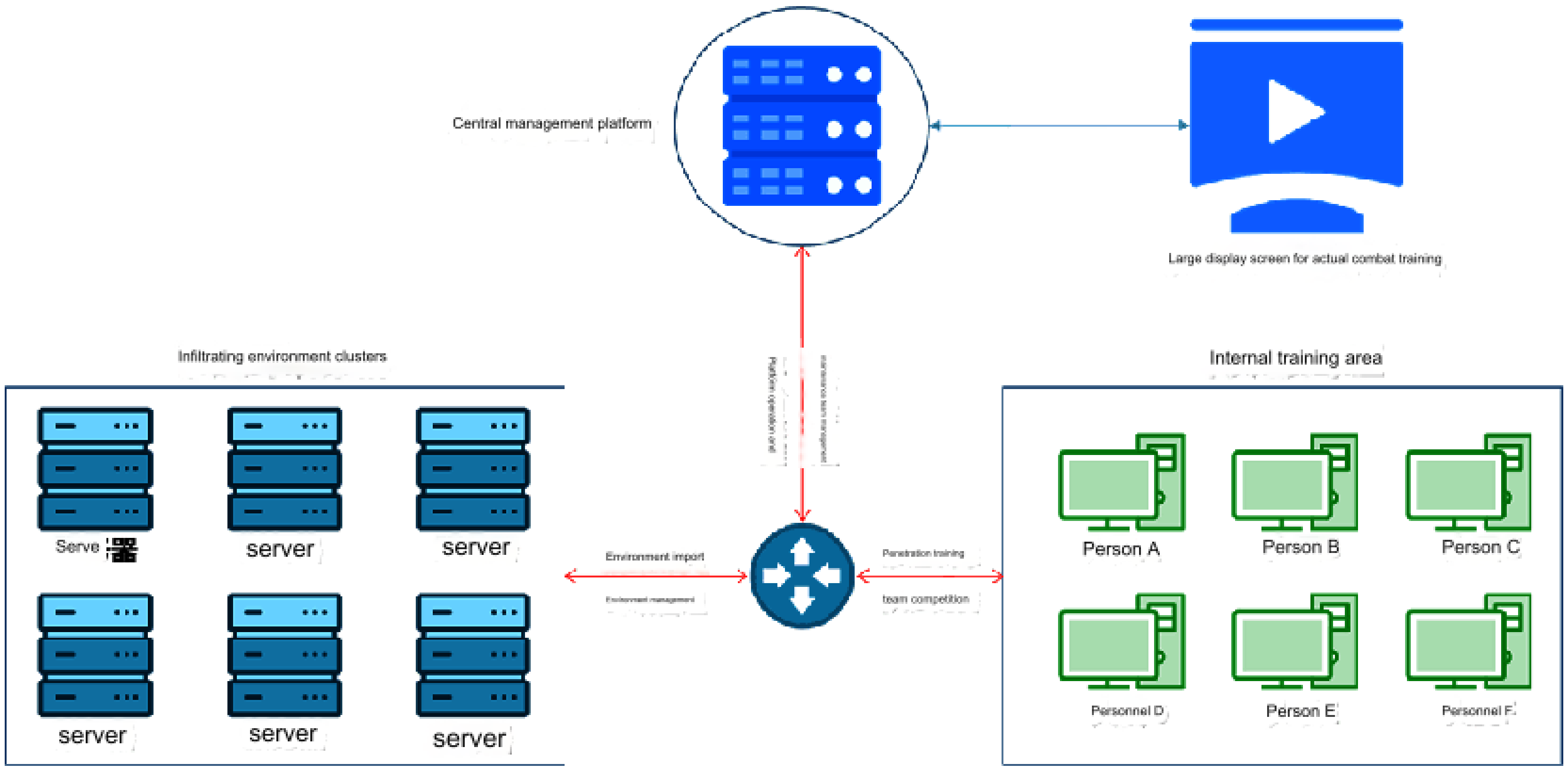
(Falcon Anti-Gambling Platform Interface Picture)

4.3 Practical training platform

4.3.1 Product Introduction

The practical training platform is based on the practical experience of network security penetration accumulated by Anxun Information for many years, combining various networks A set of professional practical training platform independently developed to meet the skill requirements of cyber security personnel by cyber investigation units.

Students can conduct real network security confrontations in a 1:1 intranet penetration environment based on actual combat scenarios to improve their practical work capabilities.



(Actual training platform operation form diagram)

4.3.2 Product functions

> Environment management: The system has built-in virtual machine templates for common websites, emails, OA and other servers. Teachers only need to select the corresponding virtual machine templates on the scene production interface to add them. This can quickly build a network simulation environment, and the platform supports customization. Transfer the target simulation environment. Through this function, you can create a network attack and defense environment that is the same as the students' real learning and work.

> Question management: Teachers can use the question management function to create new competition questions, set the name, difficulty and question type of the question. The question type fits the actual intranet vulnerabilities, including reverse engineering, vulnerability mining and utilization, Web penetration, passwords, forensics, and steganography. , safety programming and other categories to improve students' real confrontation ability and practical work ability.

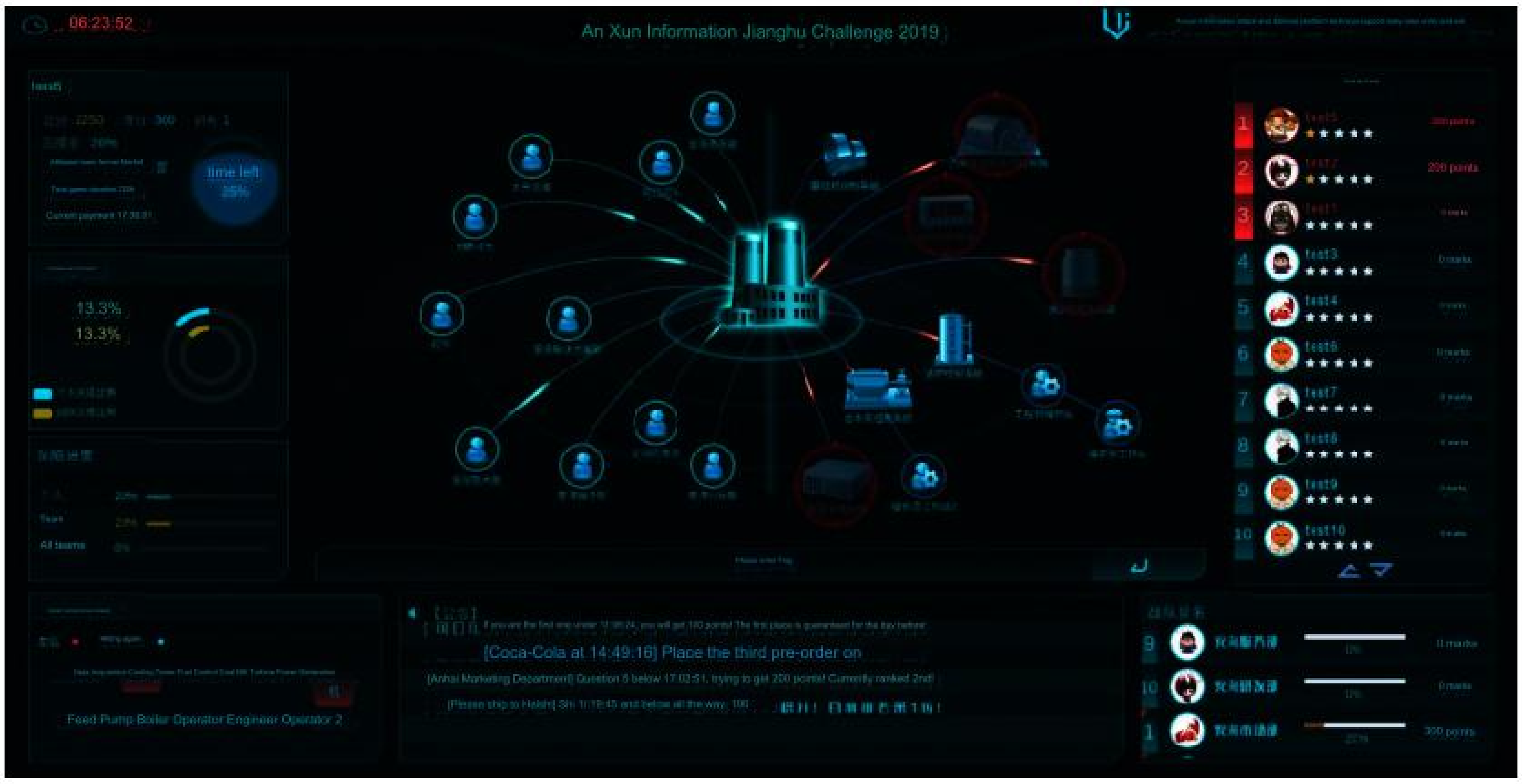
> Competition management: Teachers can use the competition management function to generate different types of test papers from the question bank and publish competitions, set the competition name, competition time, and competition rules, and can view the competition progress and results in real time.

> Team management: Supports the function of creating a team, setting the team name, team logo, and joining password. Each participating team member can join different teams through the password to conduct actual combat exercises and improve team collaboration and combat capabilities.

4.3.3 Industry advantages

- Real intranet environment——The practical-training platform is based on our company's years of experience in APT penetration attacks. It embeds the problem-solving model into the real intranet environment. On the one hand, students can submit flags by solving problems, and at the same time Based on the clues in each question, you can discover the hosts in the entire intranet for further penetration.
- Visual simulation environment customization————The platform supports users to customize the upload environment. On the one hand, it can conduct real network attack and defense training and improve students' actual working ability; on the other hand, it can also conduct scientific research on new technologies in these environments. , test, and improve the unit's network attack and defense scientific research level.
- Analysis and restoration of hot security events——The actual combat platform can simulate the real environment of hot security events, analyze and restore the events, and restore the offensive and defensive technologies involved in the events to actual combat for students.

1.3.1 Product pictures



[Coca-Cola at 14:49:16] Place the third pre-order on

[Anhui Marketing Department] Question 5 below 17:02:51, trying to get 200 points! Currently ranked 2nd!

[Please ship to Hatsh] Sh: 1:19:45 and below all the way. 190

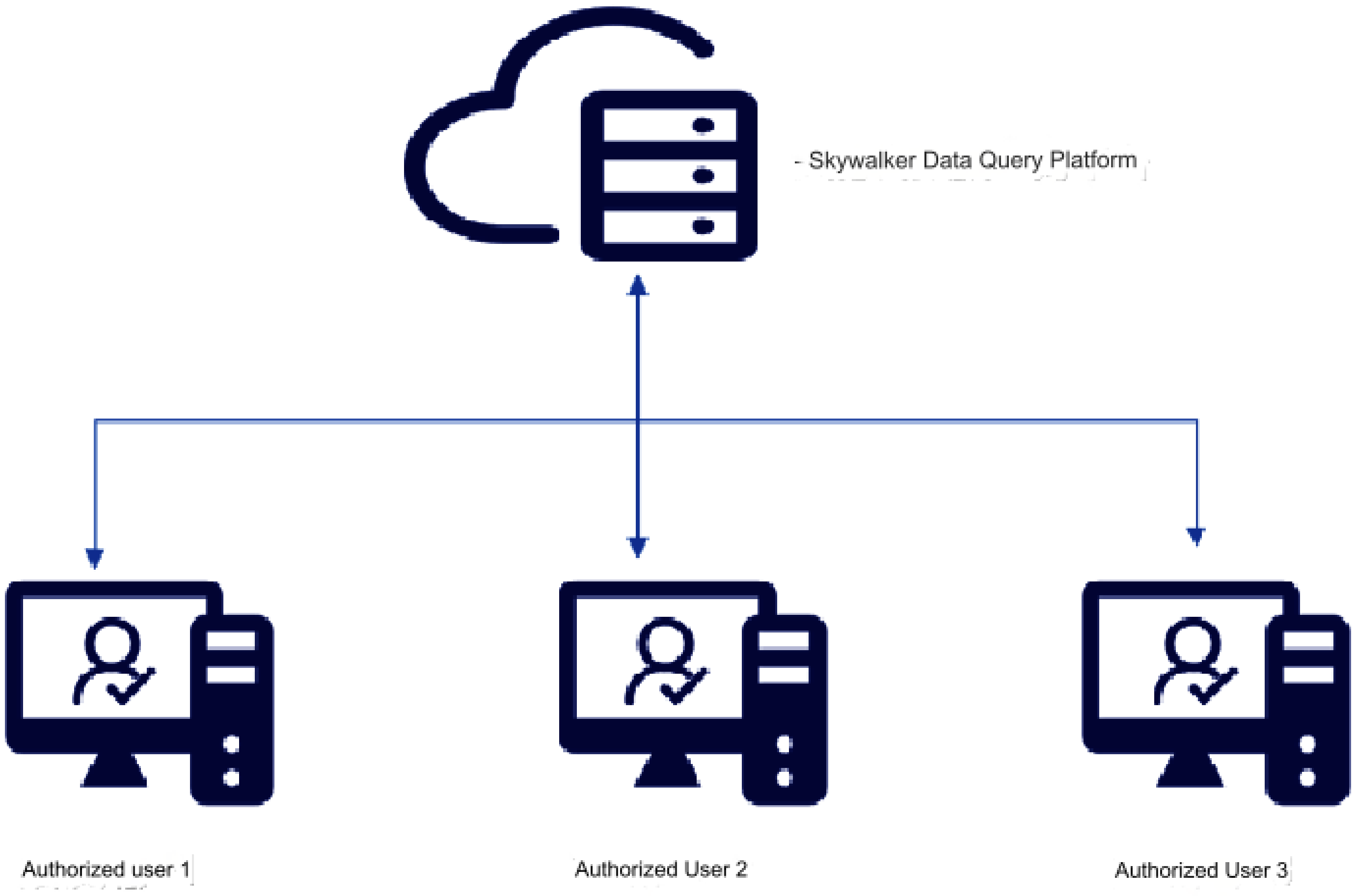
Practical training platform interface diagram

4.4 Skywalker Data Query Platform

4.4.1 Product Introduction

The Skywalker data query platform is a dedicated confidential application system that provides real-time query for target logistics information and network virtual identity information. The platform is supported by logistics information and synchronously correlates target-related information to achieve comprehensive acquisition of target person information.

The Skywalker data query platform is provided to customers for use based on cloud services. Users can log in to the system and use the functional modules of each system by authorizing the dongle.



(Operation form diagram of Skywalker data query platform)

4.4.2 Product functions

> Basic information query: Enter any keyword such as the phone number, email address, and user name of the target to be queried, and basic information such as the target's name, ID card information, household registration address, etc. can be queried.

> Logistics information query: After querying the target person's information, you can query the target's logistics information address based on the query keywords.

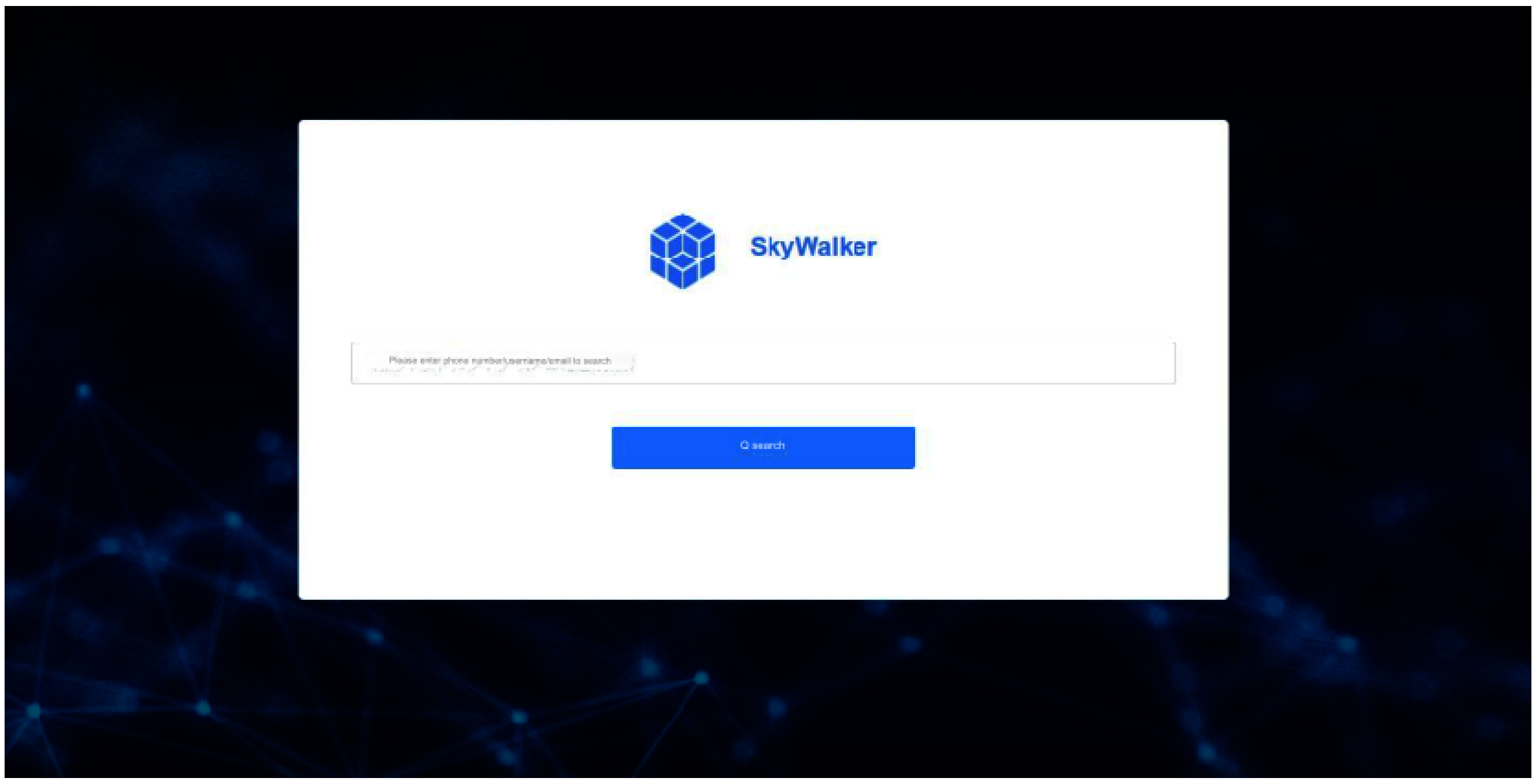
> Related data query (under development): After querying the target person's information, you can query the target's user ID, email address and other information based on the query keywords.

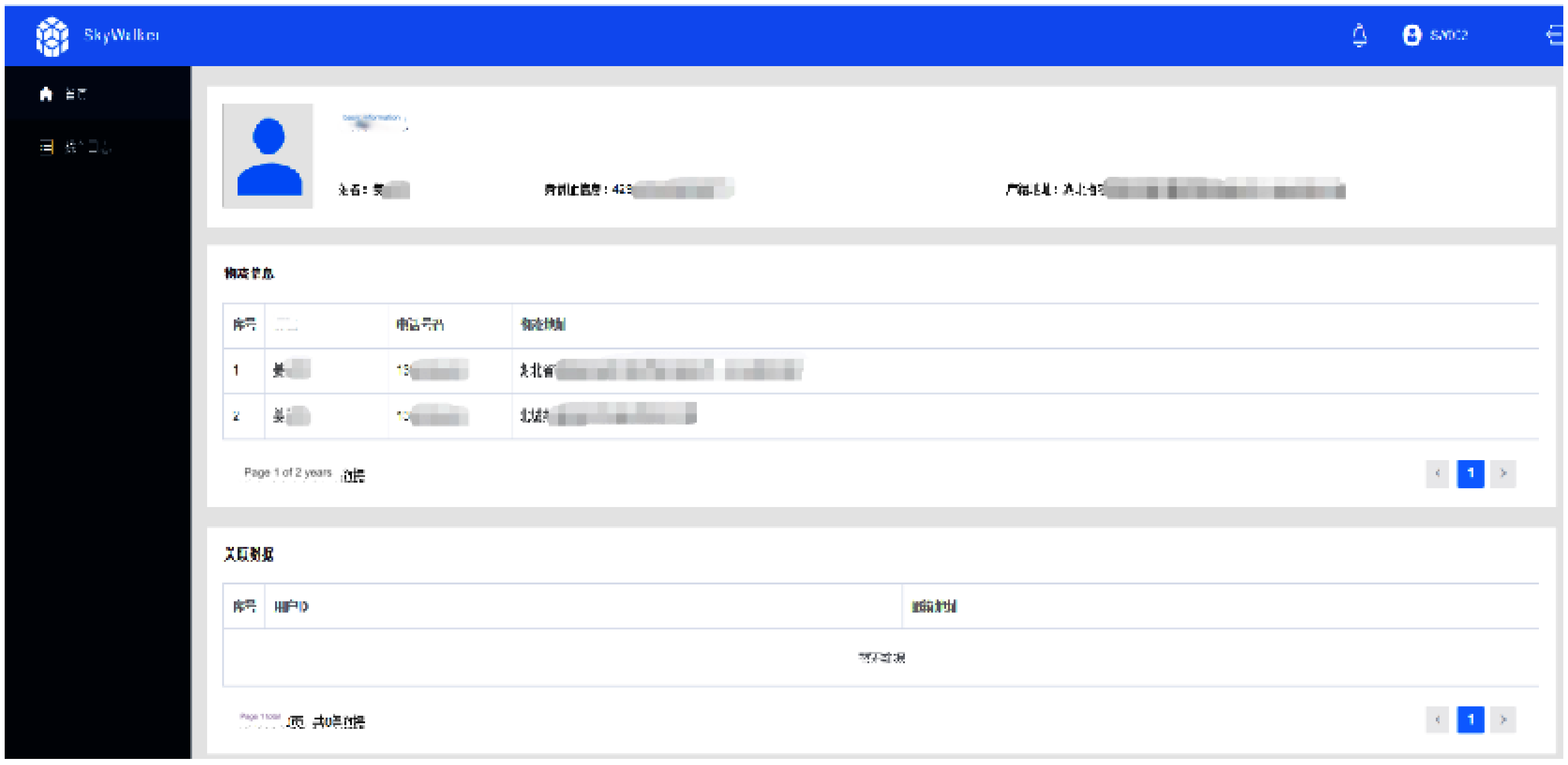
- Virtual identity query (under development): After querying the target person's information, the target's online virtual identity can be retrieved based on the query keywords, including account information such as QQ, WeChat, Sina Weibo, Facebook, and Twitter.

4.4.3 Industry advantages

- Simple operation————The interface is simple and easy to operate. Enter the target information keywords as required to obtain the query information.
- Data support——Our company's unique threat intelligence data is built into the platform to support the information investigation of relevant departments. Users can query online in real time through the Internet and quickly obtain returned information.
- High security——To ensure the security and concealment of the query, the platform adopts multi-layer encryption technology during the query process, and cooperates with USB key login to ensure the security of two-way communication between data query request and result feedback. .

4.4.4 Product pictures





SkyWalker

姓名：[redacted]　身份证号：42[redacted]　户籍地址：[redacted]

物流信息

序号	姓名	电话号码	物流地址
1	[redacted]	[redacted]	湖北省[redacted]
2	[redacted]	[redacted]	北京[redacted]

Page 1 of 2 years 数据

关联数据

序号	用户ID	注册时间
暂无数据		

共0条数据

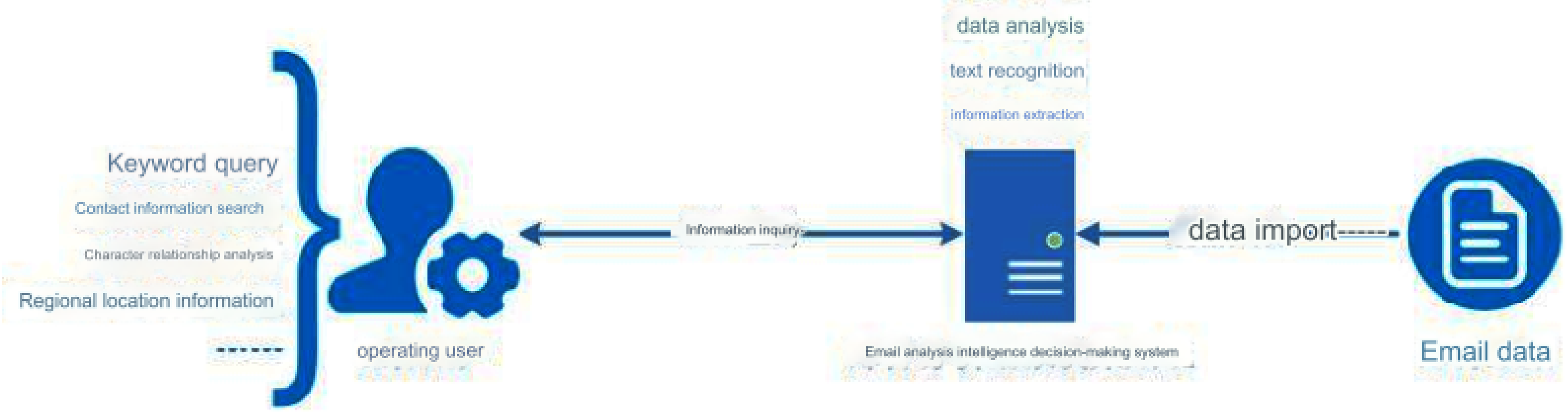
(Skywalker data query platform interface diagram)

4.5 Email analysis intelligence decision-making system

1.5.1 Product Introduction

The email analysis intelligence decision-making system is developed and designed based on text recognition big data technology. It supports the rapid identification and analysis of massive email data and extracts intelligence information such as keywords, sensitive words, personal relationships, and contact information.

The system is simple to install and deploy. You only need to deploy the application software on the server to realize the analysis and application of email big data.


data analysis
text recognition
information extraction
Keyword query
Contact information search
Character relationship analysis
Regional location information
------
operating user
Information inquiry
data import------
Email analysis intelligence decision-making system
Email data

(E-mail analysis intelligence decision-making system operation form diagram)

4.5.2 Product functions

> Automatic mail collection: The system supports automatic mail collection under SMTP, POP3, iMAP, and Exchange protocols; Exchange supports the use of non-clear text passwords for mail reception.

> Full-text quick search: The system supports quick search of email data from different data sources based on time, region, label and other conditions.

> Relationship network sorting: The system supports the description of the relationship network of the target email, including email exchange information, contact information in the email, regional geographical location information, interpersonal dimension information, etc., and can realize comparative analysis of individual targets and generate comparisons. to analysis reports.

> Early warning research and analysis: The system supports the classification and grouping management of acquired email data sources, and can combine and connect different data sources for analysis, and conduct comprehensive analysis combined with sensitive lexicon to achieve early warning research and judgment of target information.

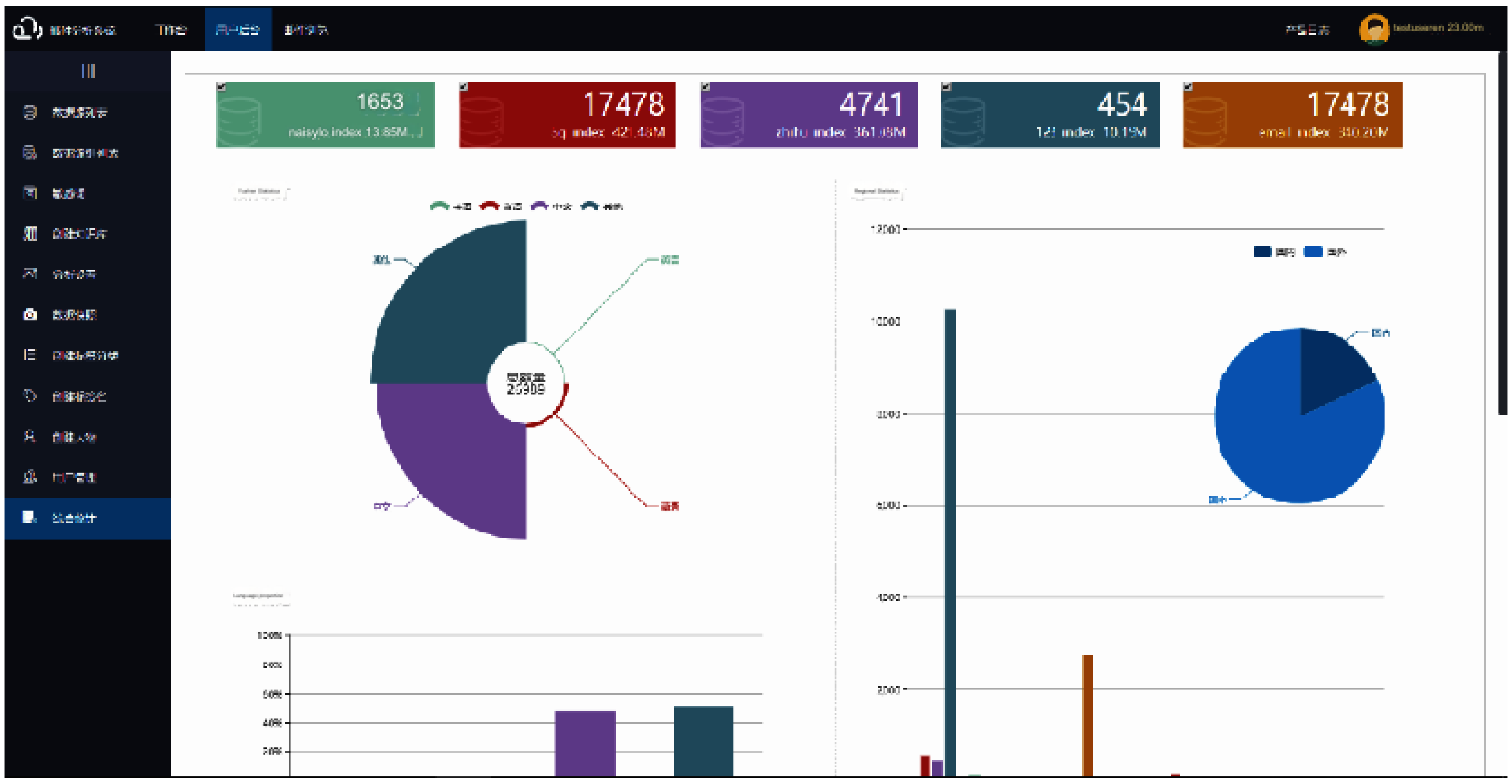
4.5.3 Product parameters

System parameters		
Server performance	operating system	Windows/Linux operating system
	CPU	Intel Xeon E5-2600 v3*2
	Memory	8G
	Hard drive capacity	2T
Browser		Requires support for HTML5
Total number of fathers		100,000 emails/station (If the server performance in the table is met, the total processing volume can increase with performance improvement)
Cluster function		Support, the performance increases linearly after adopting the moon cluster mode

4.5.4 Industry advantages

- High accuracy——The system adopts big data architecture and intelligent text recognition technology to achieve rapid analysis, accurate extraction, and rapid comparison of massive emails.
- Powerful function————The system supports various relationship analysis and value information extraction of target emails, including but not limited to email exchange information, geographical location information, communication information, activity information, etc.
- High stability——The system is stable and reliable, supporting 7*24 hours of uninterrupted operation.
- Ease of use——The system is simple to operate and adopts Caiyue graphical operation interface.

4.5.5 Product pictures



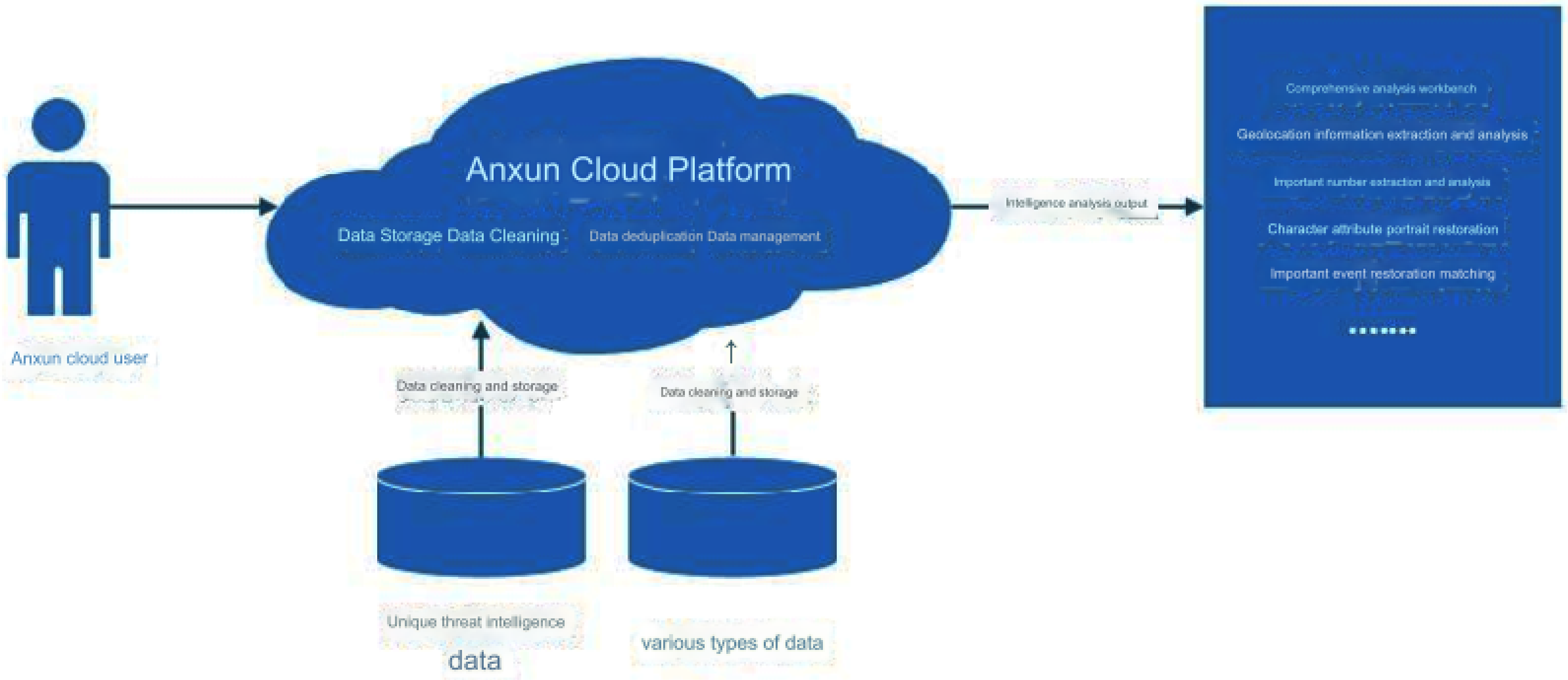
(Screenshot of email analysis intelligence decision-making system function)

4.6 Anxun cloud intelligence analysis and decision-making platform

4.6.1 Product Introduction

Anxun cloud intelligence analysis and decision-making platform is a comprehensive correlation query intelligence analysis and decision-making platform that is based on our company's unique threat intelligence data, supports the import of structured and unstructured intelligence data, and intelligently extracts and analyzes massive intelligence data.

The platform supports two application methods: one is SaaS cloud service, which allows monthly client software and authorization locks to log in to the platform to implement intelligence query, analysis and decision-making; the other is self-built private Anxun Cloud, which combines white intelligence data with Anxun Cloud Threat intelligence data has been integrated in the cloud to realize intelligence query analysis and decision-making.


Anxun cloud user
Anxun Cloud Platform
Data Storage Data Cleaning
Data deduplication Data management
Intelligence analysis output
Comprehensive analysis workbench
Geolocation information extraction and analysis
Important number extraction and analysis
Character attribute portrait restoration
Important event restoration matching
·······
Data cleaning and storage
Data cleaning and storage
Unique threat intelligence
data
various types of data

(Anxun cloud intelligence analysis and decision-making platform operation form diagram)

4.6.2 Product functions

> Data cleaning and warehousing: The platform has built-in unique communication threat intelligence data. It can also be combined with the user's own intelligence data to import and analyze information data in various formats, including: structured data such as databases and unstructured data such as documents and pictures. Data Format.

> In-depth relationship analysis: Based on the powerful algorithm capabilities of the platform, different algorithm models can be selected according to different data sources to conduct in-depth analysis of the relationships of massive data. It supports automatic face detection, similar picture search, document recognition, etc., providing users with Provide comprehensive communications intelligence and decision-making information.

> Deep mining of data intelligence: Through in-depth analysis of massive data, the platform further mines intelligence to achieve extraction and decryption of the target's geographical location, important numbers, suspected accounts, restoration of important events, restoration of character attribute portraits, intelligence popularity, and sensitivity Word mining and other aspects of data mining.

4.6.3 Product parameters

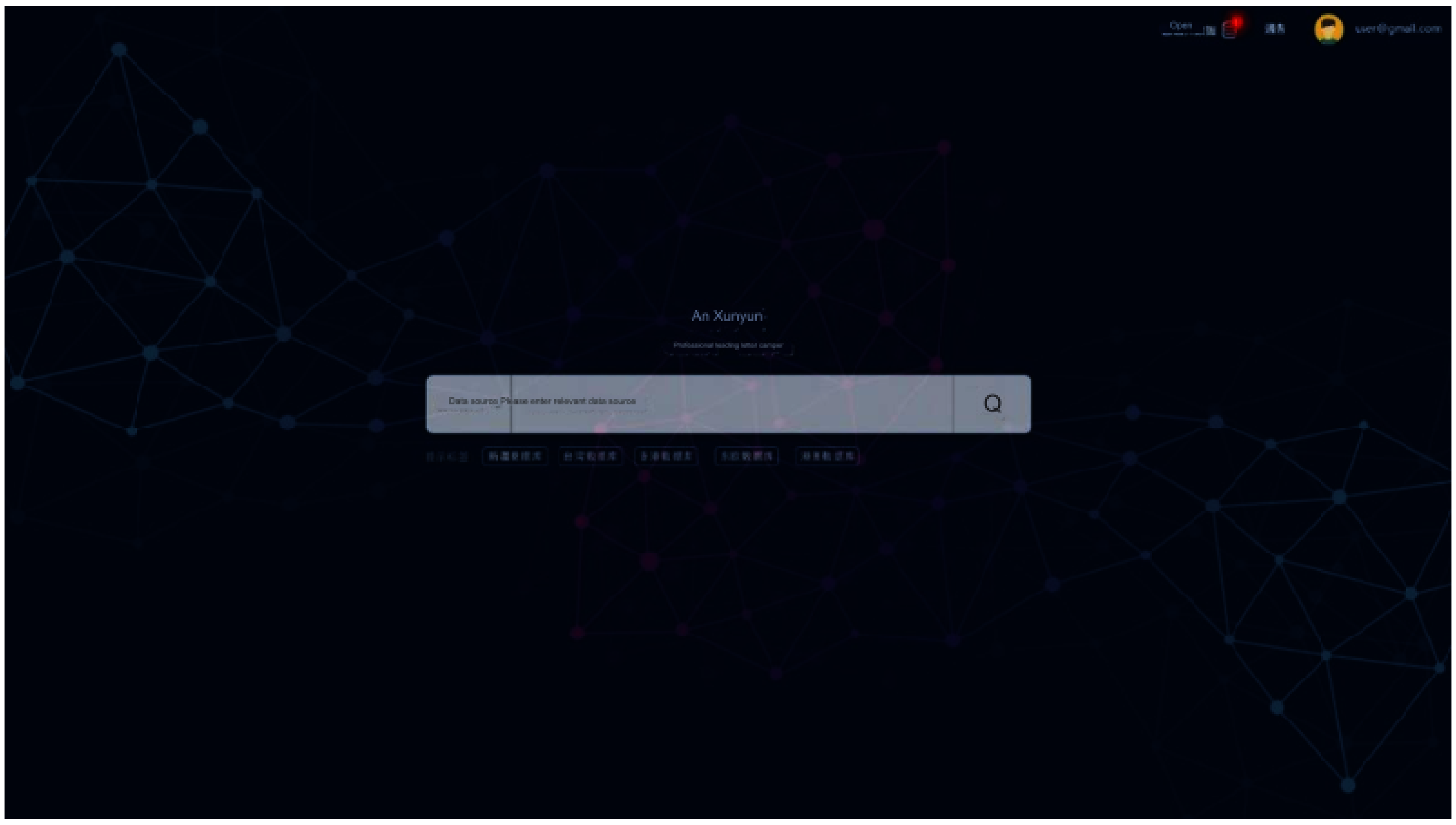
project	parameter
Provide data volume	PB-level massive data capacity storage
Data processing volume	Petabytes of data
Data analysis processing speed	Second level
Data import speed	Second level
Password cracking speed	Second level

Sensitive word statistics	Multiple categories, support customization

4.6.4 Industry advantages

- High scalability——The platform can provide application extension API interfaces based on user business needs to enrich and extend applications.
- High accuracy——The platform supports precise retrieval of single or multiple conditions of the target within seconds to obtain target information.
- Excellent comprehensiveness——The platform supports the analysis and calculation of multiple data sources (email data, communication data, social data), and the platform has built-in Anxun Information's unique intelligence data to fully grasp the data intelligence relationship.
- High convenience——The platform is based on deep learning technology and can quickly extract and analyze massive data, making it highly efficient and convenient.
- Ease of use——The platform is easy to deploy and install and easy to operate.

4.6.5 Product pictures


Open
user@gmail.com
An Xunyun
Professional leading letter camper
Data source
Please enter relevant data source

(Anxun cloud intelligence analysis and decision-making platform interface diagram)

Summary of front-end sales feedback issues

1. The speed of the company's self-developed products has declined, there is no continuous update, and the iterative update of equipment is too slow. The company has been providing services in recent years;

2. QB data does not have good points;

3. The company's products are offline, front-end sales are unclear and there is a lack of communication;

4. In terms of delivery, there is a lack of communication between the back-end and the front-end, and there are many problems in delivery;

5. Poor delivery quality, poor settlement, and accumulation of accounts receivable affect cash flow;

6. The company does not have channel suppliers for unified products, and does not know which supplier's products to recommend when selling;

7. Anxun Academy has not been updated for a long time, and there is no training, which has a certain negative impact on Anxun's brand, and customers doubt whether the company is operating normally;

8. The testing of new products after they were launched was very unsatisfactory (assistant investigation platform and talent empowerment platform). Customers were interested in the anti-fraud publicity toolbox, but the product could not be launched for a long time;

9. There are big problems with the sales process. Many complicated processes need to be submitted to coordinate the work. The collaborative work efficiency is too low and internal friction is serious;

10. The PPT is too long and the customers cannot understand it. The district and county PPT can be modified.

11. The sales project contract is difficult to find, and the node review is complicated. After the salesperson leaves, it is difficult for the new employee to connect with the work. It is recommended to use the sales CRM system to improve work efficiency and standardize the sales process. This work is currently being followed up by Li Zhengxia.

Anonymous anti-tracing wall quotation

serial number	product name		Functions and parameters	quantity	Remark
1. Software part					
1	"Anonymous anti-tracing wall" system	Internet setting module	1. Supports DHCP, static IP and dial-up Internet access; 2 ·Supports restarting or shutting down ANS services and replacing ANS nodes.	1	Provide a one-year free upgrade and update service for the entire system-related software
		Anonymous service module	It can provide two anonymous links, anonymous service and onion network, to flexibly choose anonymous Internet access methods.		
		NATC service module	It can provide users with port mapping services. Through user-defined port mapping rules, the IP port in the "Anonymous Anti-Tracing Wall" device can be mapped to the port of the specified server IP.		
		Dark web access module	1. Support access to private network-specific Shensuanzi and Anxun Cloud dark network QB information platforms; 2. Supports accessing all dark web resources on the public network through a specific browser.		
2. Hardware part					
2	"Anonymous anti-tracing wall"		1. Architecture: ARM 2.Length, width and height 28.2*16.1*4.3(cm) 3.CPU: Dual-core 800MHz 4. Memory: 512MB DDR3 5.4 10/100M adaptive LAN 6.1 10/100M adaptive WAN □ 7.1 power input ports 8. .4G Internet access: supported	1	Provide one-year free maintenance service for the entire system-related hardware
	Total price		RMB (uppercase): one hundred and twenty thousand yuan		

illustrate: 1. The above prices include tax, with a tax rate of 13%;

2. The product provides free after-sales maintenance services for one year from the date of delivery;

3. The renewal amount for the second year is RMB 1,120,000.