SecureIQlab®

Threat Research Report

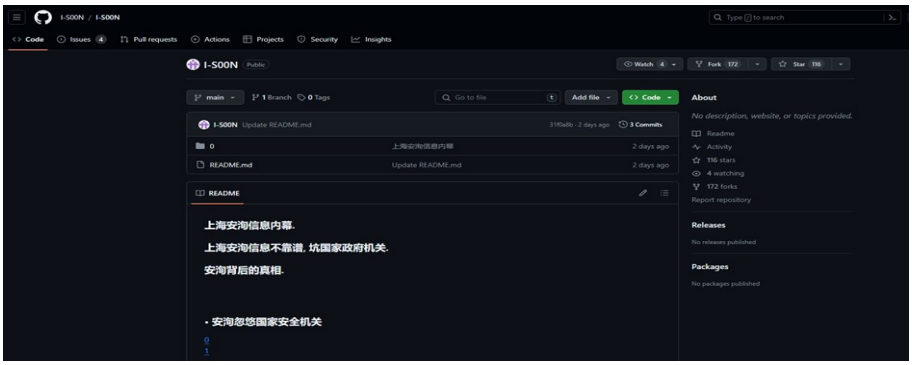
Hacking Firm I-Soon Data Leak Reveals Chinese Government Hacking Capabilities

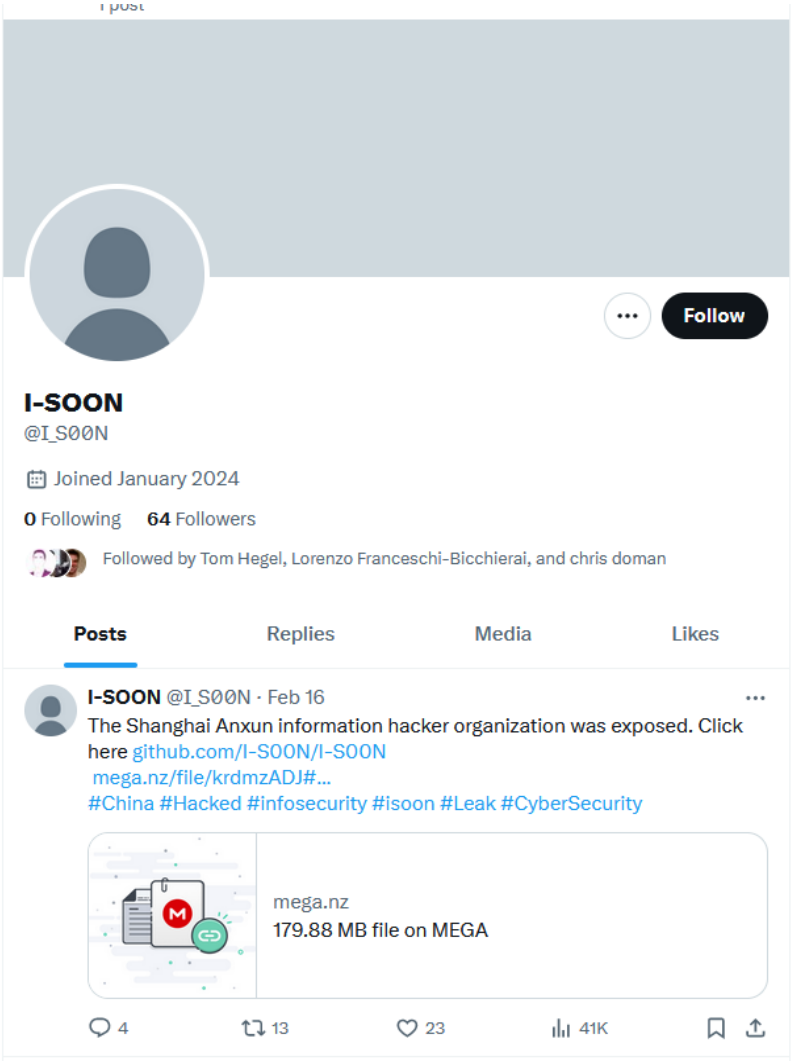
Published: 26 March 2024

Table of Contents

1. Introduction

On February 16, 2024, an unidentified person/group published a significant amount of data on GitHub. The treasure trove of confidential information resulted from a breach of the China-based company iSoon, also known as Anxun, a contracted entity associated with the Chinese Ministry of Public Security (MPS). The incident is reportedly linked to Chengdu 404, a structure under the control of Chinese cyber intelligence, famously recognized as APT41.





The leak sheds light on the forms and methods of Chinese intelligence, revealing a range of tools and techniques. These include software, Trojans designed for Windows, Mac, iOS, and Android platforms, DDoS services, systems for de-anonymizing social network users, Wi-Fi hacking equipment, and more. The disclosed information encompasses a wealth of details about penetration and information acquisition methods.

The attackers targeted both general information, such as databases, and specific individuals' information, including control of correspondence, calls, and movement. Data analysis revealed that the compromised information amounted to a substantial volume, measured in terabytes, and underscored the magnitude of the security breach. The data obtained from the breach shows critical infrastructure targets in countries including Nepal, India, France, Kazakhstan, Kyrgyzstan, Mongolia, Pakistan, Malaysia, Turkey, Egypt, Cambodia, Rwanda, Nigeria, Hong Kong, Indonesia, Vietnam, Myanmar, the Philippines, and Afghanistan.

Find all the victim lists here.

This data breach illuminates the intricate forms and methodologies Chinese intelligence utilizes, providing valuable insights into their operational strategies.

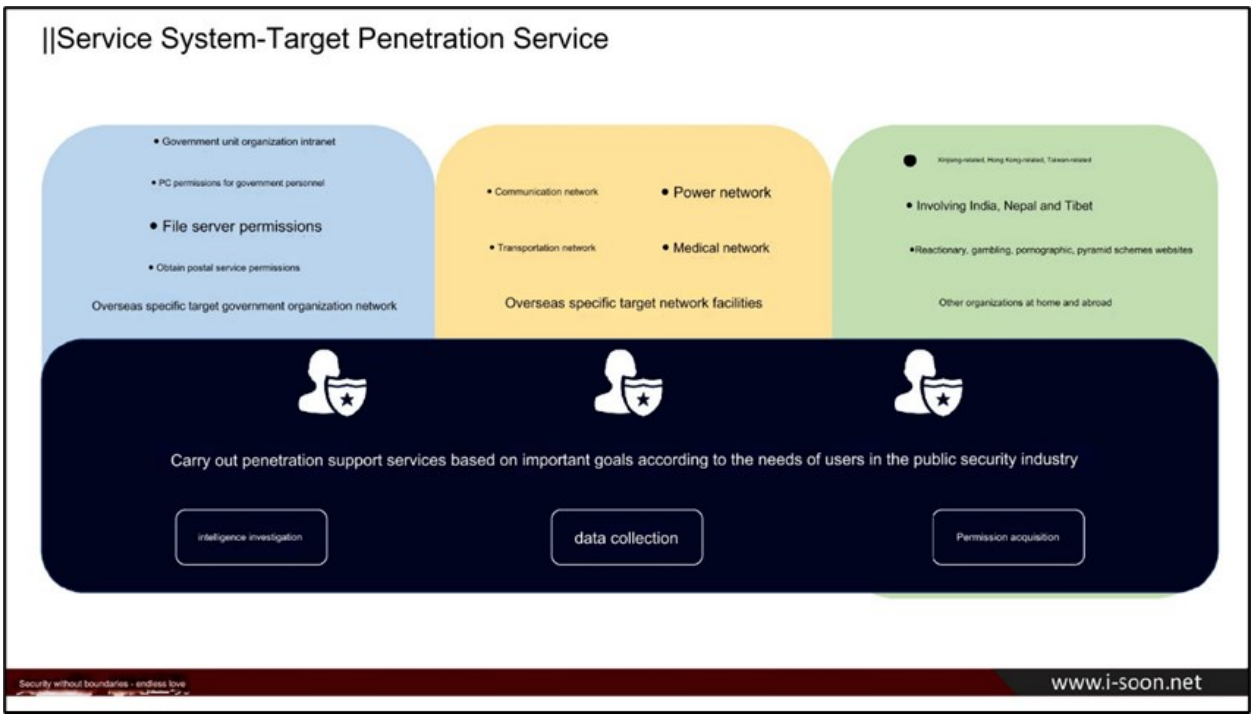
2. I-SOON Briefing

As a leaked iSOON presentation revealed, the company's organizational structure comprises three penetration teams, a security research team, and a basic support team, totaling approximately 70 personnel.

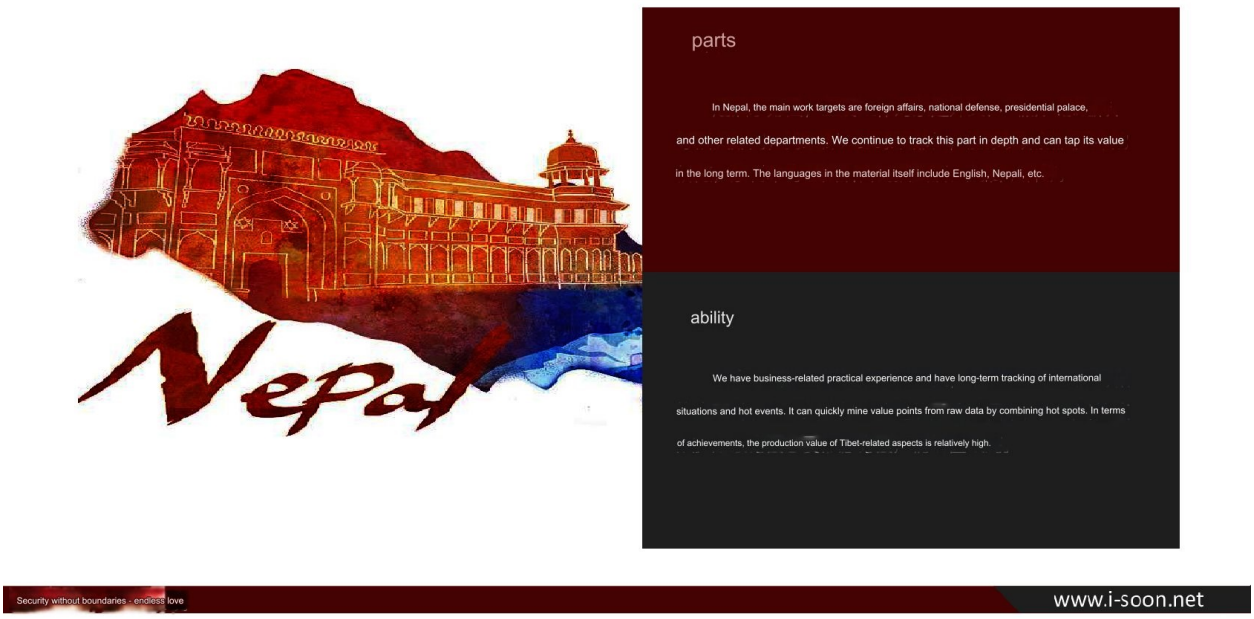
ISOON's operations primarily focus on specific countries and regions, including Central Asia, Southeast Asia, Hong Kong, Macao, and Taiwan. Among the services offered to their MPS clients are "APT Service System," "Target Penetration Services," and "Battle Support Services."

Their scope of operations extends to various regions within China, such as Xinjiang and Tibet, where iSOON has reportedly targeted dissidents, illegal gambling rings, illegal pornography rings, and illegal pyramid schemes, all falling under the jurisdiction of MPS.

Noteworthy is iSOON's inclusion in a slide deck detailing their cyber-attacks on the governments of India and Nepal. These attacks specifically targeted government departments such as the Ministry of Foreign Affairs, Defense, Home Affairs, Finance, and the Nepalese Presidential Palace.



|| Intelligence Service-Shenni



3. Technical Details of the Leak

Among the materials is documentation and description of spyware programs designed for monitoring and collecting information in real-time, with the ability to gain full access to devices.

In other instances, technical documents showcased to prospective clients detailed the operational methods of the company's products in compromising and exploiting targets. The documentation included images of specialized hardware snooping devices, such as a disguised power bank that covertly transmitted data from the victim's network to the hackers. Additional documents provided diagrams illustrating some of the inner mechanisms of iSOON's offensive toolkit. While the capabilities were neither surprising nor extravagant, they affirmed that the company's primary revenue stream is derived from hacking-for-hire and offensive capabilities.

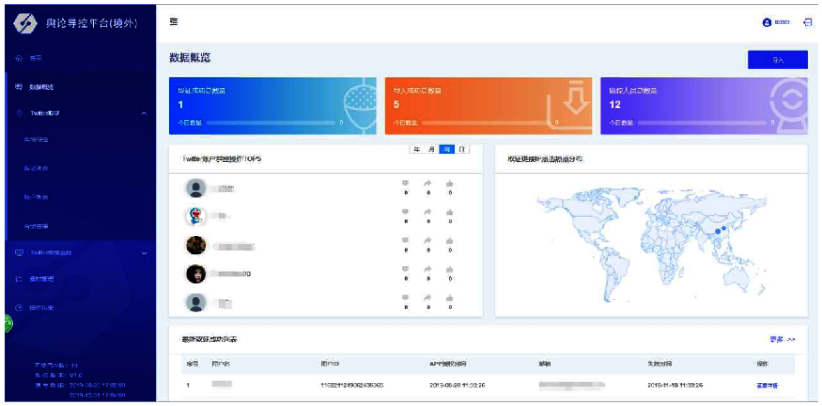
ISOON offers the following range of products and tools:

A. **Twitter Public Opinion Guidance and Control System**
B. **Email Analysis Intelligence Decision-Making Platform**
C. **Automated Penetration Testing Platform**
D. **Skywalker**
E. **DDoS system**
F. **Windows Remote control management system**
G. **Mac Windows Remote control management system**
H. **iOS Windows Remote control management system**
I. **Android Windows Remote control management system**
J. **Linux Windows Remote control management system**
K. **WIFI Proximity attack system**

A. Twitter Public Opinion Guidance and Control System

The leaked document mentions that the Twitter Tool whitepaper served as a promotional tool for iSOON to market its commercial surveillance platform to the Chinese MPS, specifically for monitoring dissenting voices. Notably, iSOON developers asserted the possession of a 1-click exploit designed to circumvent Twitter's two-factor authentication (2FA) security measures, enabling them to take control of the target's account. This exploit was intended for distribution through Twitter direct messages (DMs) in the form of URLs, referred to by iSOON as forensic links. These forensic links provided access to the targeted accounts and collected information such as IP addresses, IP locations, device type, and browser version.

The Twitter Tool whitepaper provided a comprehensive breakdown of the methods employed by Chinese intelligence services to access Western social media platforms while circumventing the Great Firewall of China. This platform empowered the Chinese MPS to scrutinize tweets and Twitter account profiles belonging to targeted dissidents. Operators within the Chinese MPS, utilizing the iSOON platform, could gather "evidence" through the platform's collection system. This system involved indexing content from Twitter users who expressed criticism of the Chinese Government.



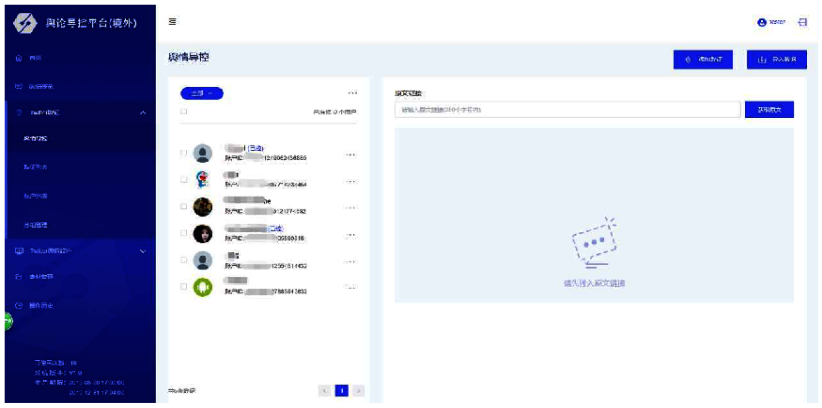
（数据概览）

4.3 Twitter 账号取证

用户通过平台获取到取证链接，通过对目标人物进行贴靠，投放链接，诱导目标点击取证链接，点击成功后，即可获取到目标 Twitter 账户权限，实现对目标 Twitter 账户的反制功能，通过 Twitter 舆情导控系统获取到目标 Twitter 账户发表推文、查看私信、评论推文、转发推文、点赞推文等综合权限，如无需在对目标 Twitter 账号进行监控，则可将目标从平台删除。

4.3.1 舆情导控

进入系统，选择舆情导控，针对已控的 Twitter 账户，选中一个或多个已控账号，输入需要进行舆论导控的推文，获取原文，选择操作评论、转发、点赞。如下图所示：



（舆情导控）

B. Email Analysis Intelligence Decision-Making Platform

iSOON marketed its Email Analysis Intelligence Platform to the Chinese MPS, aiding intelligence production by analyzing extensive volumes of pilfered emails. The platform was specifically crafted for large-scale scrutiny of email data, which allowed for the extraction of personal information, IP addresses from email headers, and details from email attachments. With the capability to handle terabytes of email data, it boasted advanced features such as indexing for keyword searches and automatic translation of emails from any language.

专业的数字情报解决方案提供商

敏感词统计	多种类，支持自定义

4.6.4 行业优势

- 扩展性高——平台可结合用户业务需求，提供应用扩展 API 接口，丰富扩展应用。
- 精准性高——平台支持对目标的单一条件或多条件的秒级精准检索，获取目标信息。
- 全面性佳——平台支持多种数据源（邮件数据、通联数据、社交数据）的分析计算，并且平台内置安洵信息独有情报数据，全面掌握数据情报关系。
- 便捷性高——平台基于深度学习技术，对海量数据快速提取分析，使其具有高效率性和便利性。
- 易用性强——平台部署安装方便，操作简单。

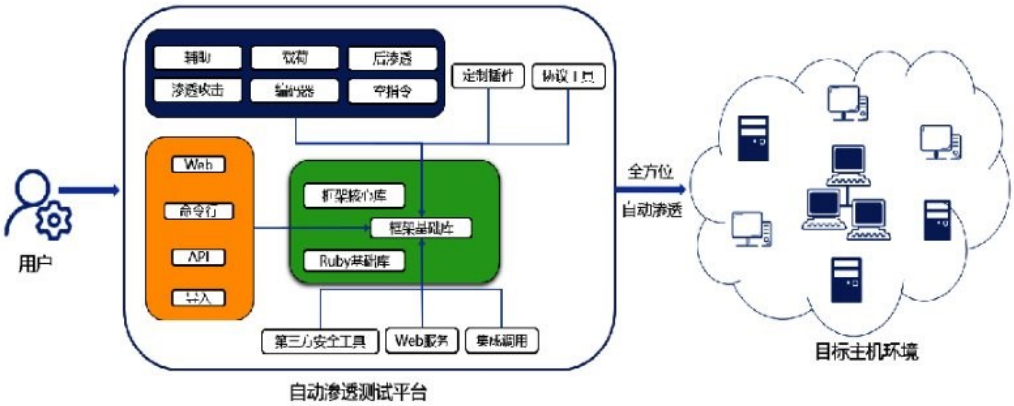
4.6.5 产品图片

（安洵云情报分析决策平台界面图）

安洵信息技术有限公司 50/50

C. Automated Penetration Testing Platform

iSOON has created an additional platform for the Chinese MPS, employed in conducting offensive cyber operations against a diverse set of targets, similar to those outlined in the iSOON services section above. This automated penetration testing platform comprises multiple modules crafted with custom and publicly accessible tools. It provides a range of offensive techniques, as detailed below, encompassing activities like executing phishing campaigns, exploiting applications, generating cross-platform payloads, and deploying RATs (Remote Access Trojans), which may include legitimate remote monitoring and management (RMM) tools.



（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。

D. Skywalker

The leaked document has also mentioned a tool named Skywalker, a data research platform used to search for information associated with a given keyword, such as phone numbers, email addresses, and usernames, subsequently revealing the real-life details of the individuals.

- **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

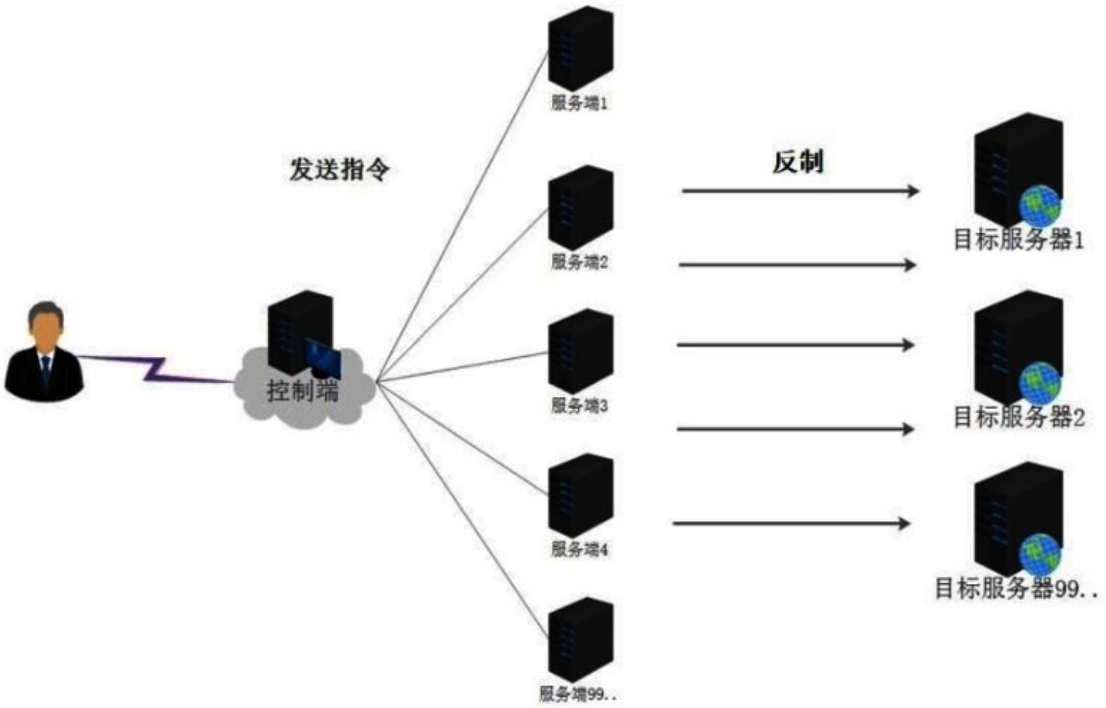
E. DDOS System

The leaked document also indicated the presence of a DDoS system. The botnet client has a size of 29 KB and is deployable on Windows, Linux, or generic IoT devices, boasting a total throughput ranging from 10 to 100 Gbps.

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）

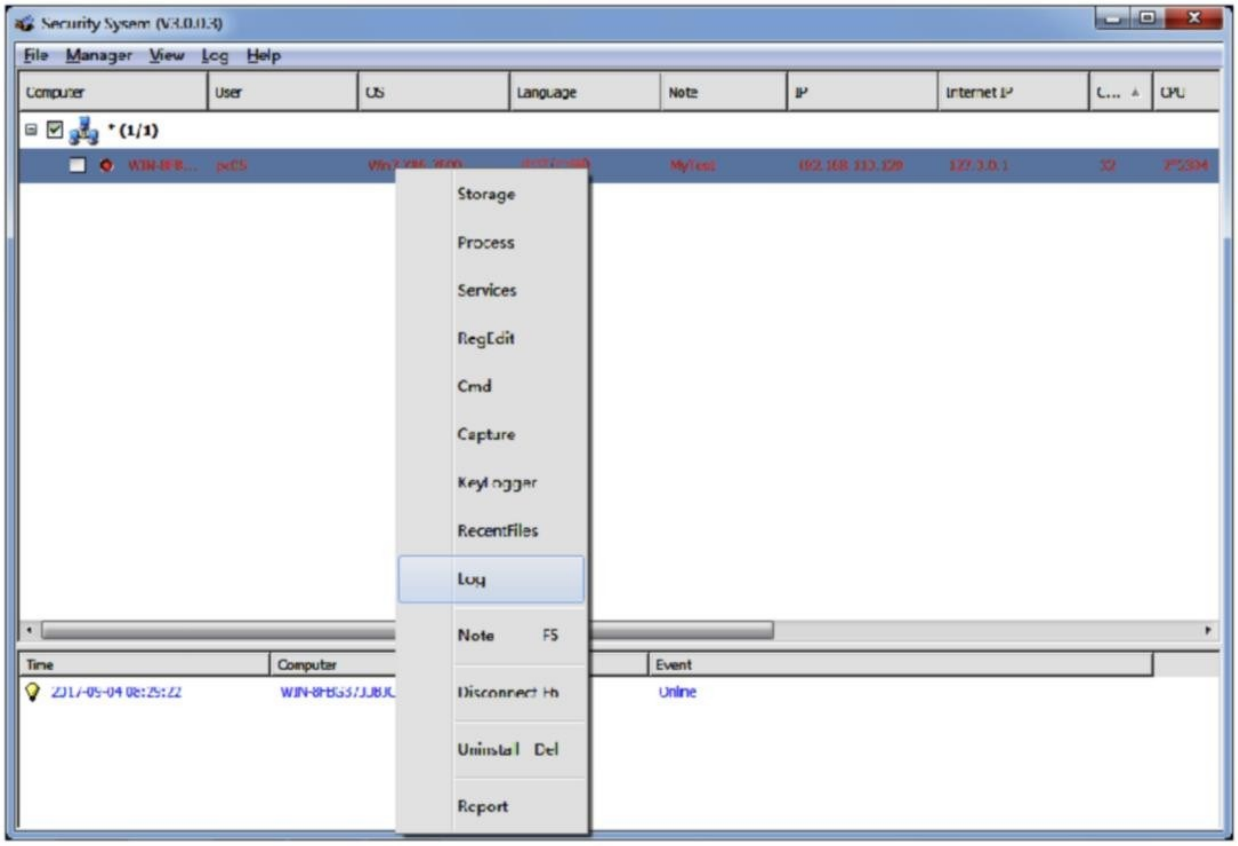
系统为 C/S 和 B/S 架构并存，充分吸收两种架构的特点。反制流量获取模块采用主动式扫描获取技术，获取全球存活网络流量并且进行综合性自动化海量漏洞探测，实现为反制流量控制模块提供网络流量数据。

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。

F. Windows Remote control management system

- The Remote Access Trojan for Windows x64/x86 can retrieve all information about the host, manage processes, manage files (view, delete, execute, change), execute commands (CMD operations), take screenshots, employ a KEYLOGGER (records every key pressed on the keyboard), and much more.

The cyber espionage group claims that 95% of antivirus programs, including Kaspersky, Symantec, and other popular solutions, will be unable to detect this Trojan. The Trojan can remove itself and start autonomously.

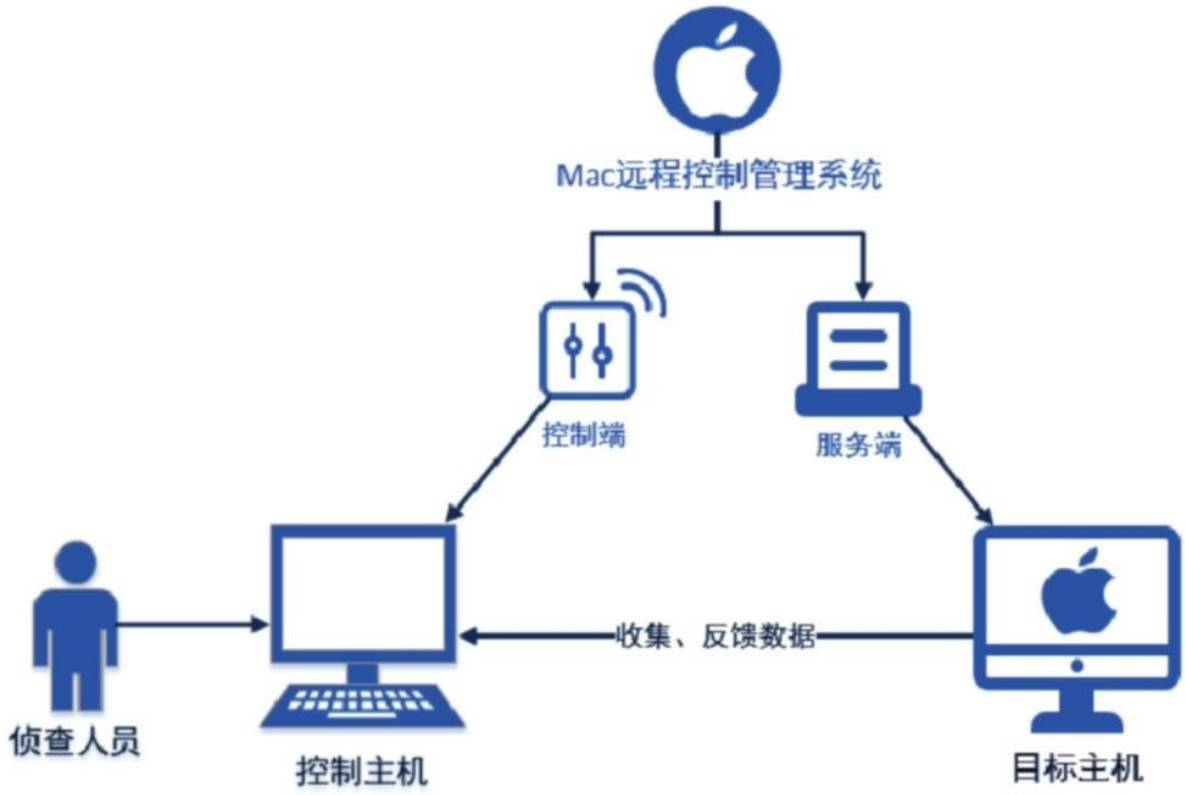


（Windows 远程控制管理系统界面图）

Windows Remote Control Management System Interface

G. Mac OS Windows Remote control management system

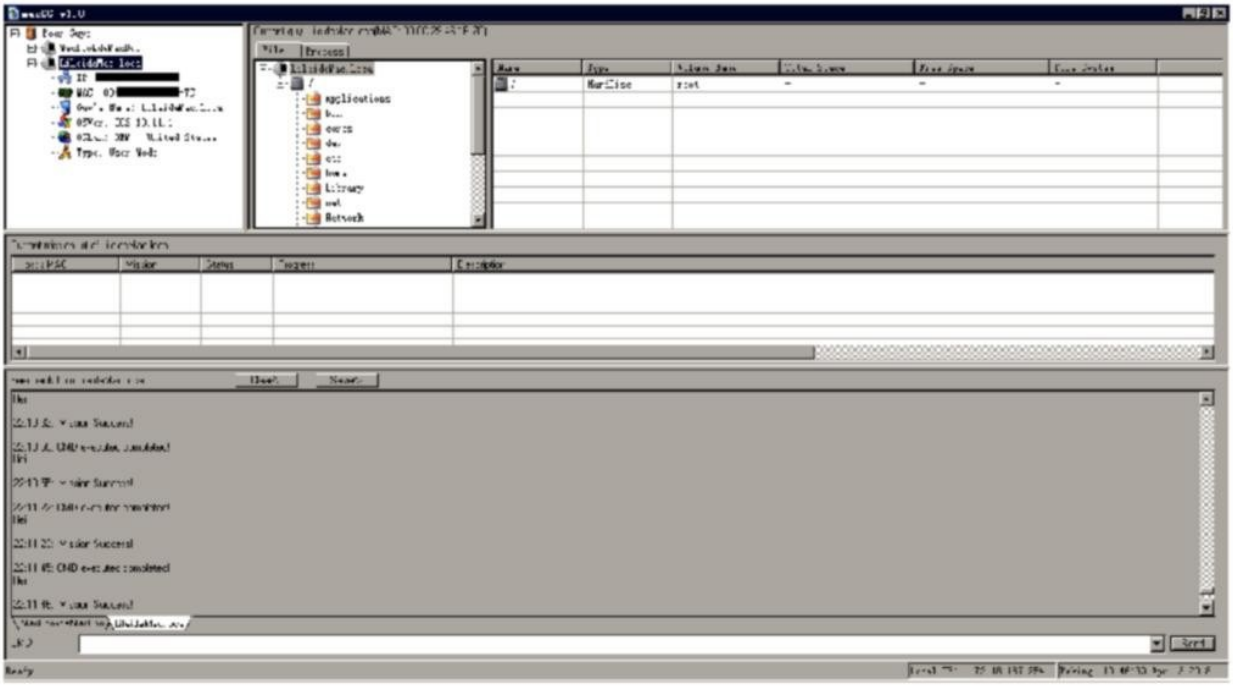
Mac also has a version of the Trojan for keylogging, screen recording, file management, executing shell commands, etc. The cyber espionage groups state that the Trojan supports all versions of Apple OS and has self-recovery functionality.



（Mac 远程控制管理系统运行形态图）

Mac Remote control management system operation diagram

1.4.5 产品图片



（Mac 远程控制管理系统界面图）

Mac Remote control management system interface diagram

H. iOS Remote control management system

The cyber espionage group also claims functionality for iOS across all versions. The features include:

- IP address collection
- GPS location tracking
- Collecting the user's complete contact list
- Multimedia collection
- Recording the user's screen ko

（iOS 远程控制管理系统运行形态图）

iOS remote control management system operation diagram

1.5.5 产品图片

（iOS 远程控制管理系统界面图）

iOS Remote control management system interface diagram

I. Android Remote Control Management System

The cyber espionage group claims that there is a version for Android (from Android 6.0 and higher).

RAT functionality includes:

- Collection of all information about the phone (device name, phone number, IMEI, CPU information, etc.)
- Collection of the entire contact list
- Collection of all call details (recipient, duration, analysis, etc.)

- Collection of all files (music, video, photos, documents, etc.)
- Keyboard monitoring
- Screenshots
- Wi-Fi information (SSID, MAC address, signal strength, etc.)
- Uploading messages from QQ, WeChat, and MoMo (root access required)
- Keylogging specifically for QQ, WeChat, MoMo, and Telegram (root rights required)

1.6.5 产品图片

（Android 远程控制管理系统界面图）

Android Remote control management system interface diagram

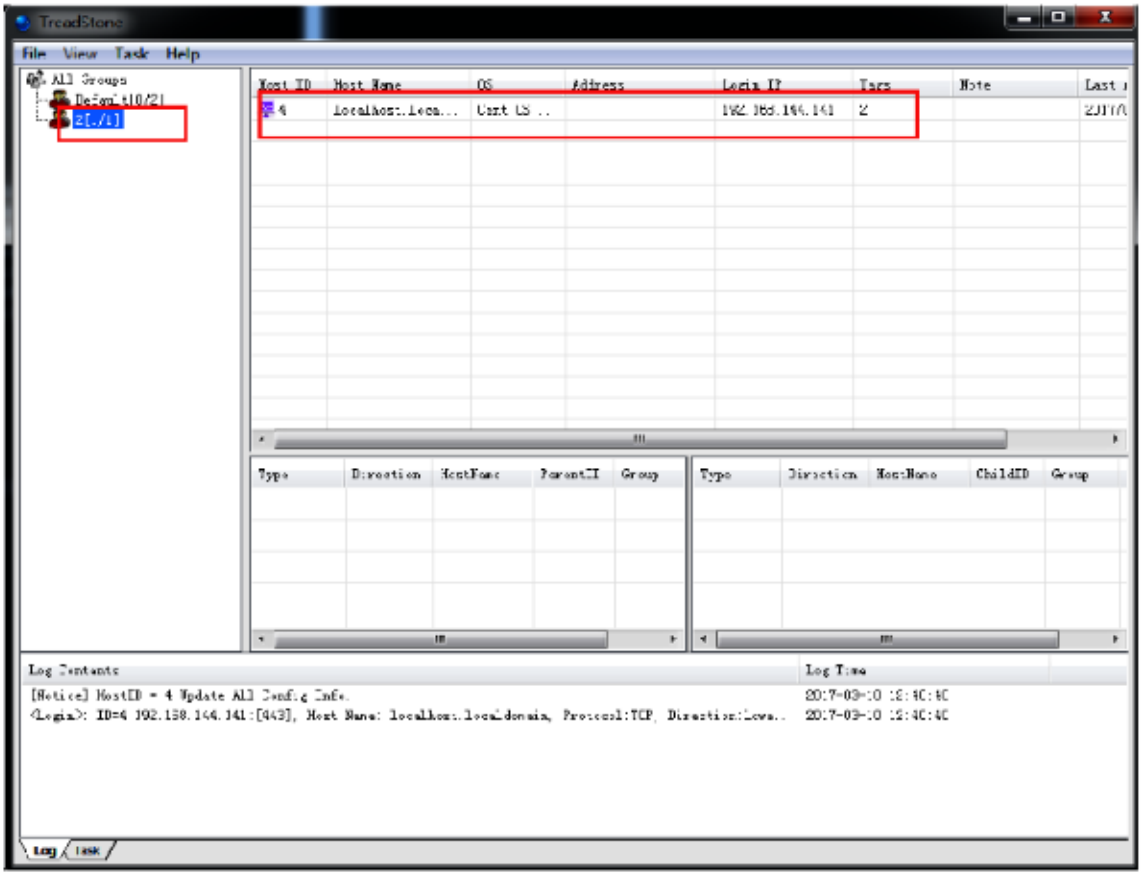
J. Linux Remote Control Management System

The cyber espionage group claims a version available for Linux, which also supports CentOS 5/6/7 and Ubuntu 12/14.

RAT functionality includes:

- Running shell commands as the user
- File management (viewing, deleting, downloading, etc.)
- Support for Socks5 proxy server
- Support for TCP port multiplexing

1.7.5 产品图片



（Linux 远程控制系统界面图）

K. WIFI Proximity Attack System

The cyber espionage groups claim that they have developed the Wi-Fi Proximity Attack System based on near-field proximity attacks, achieving the remote control of nearby devices to penetrate the target intranet. It enhances the concealment, convenience, and accuracy of penetration.

The system is divided into the Wi-Fi Proximity Attack System (basic version) and the Wi-Fi Proximity Attack System (mini version).

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

The regular version resembles the popular Xiaomi Wireless Battery:

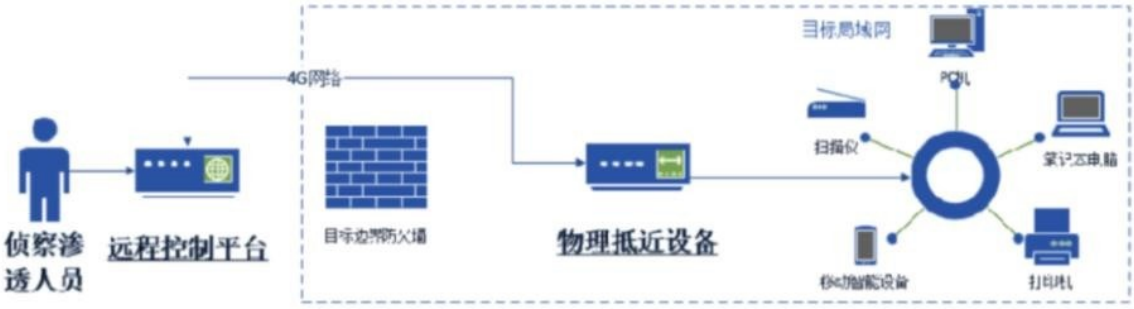
2.1 WiFi 抵近攻击系统

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）

Wi-Fi Proximity Attack System (basic version)

2.1.5 产品图片

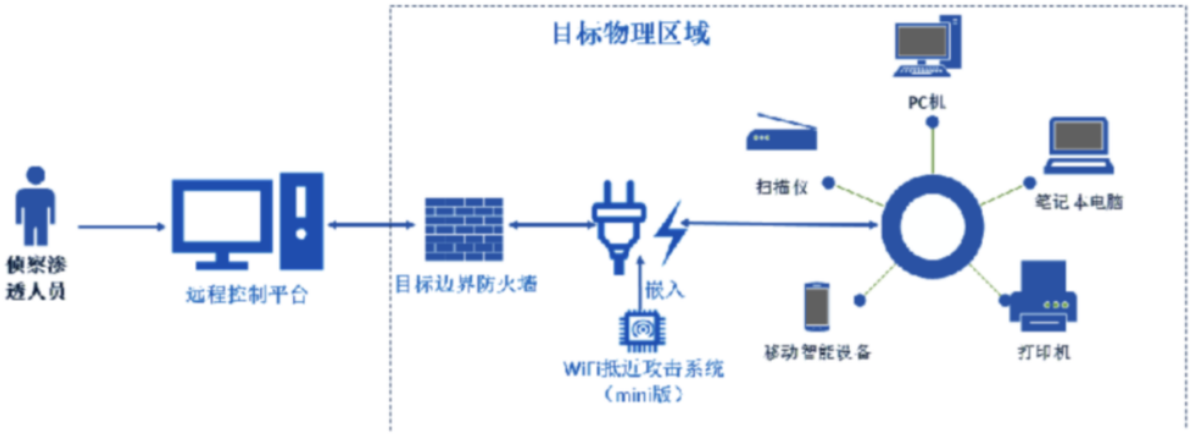
（WiFi 抵近攻击系统（基础版）产品实物图）

Wi-Fi Proximity Attack System (basic version product)

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 Wi-Fi in the target area. It establishes a SOCKS proxy tunnel to achieve close penetration of the target network.

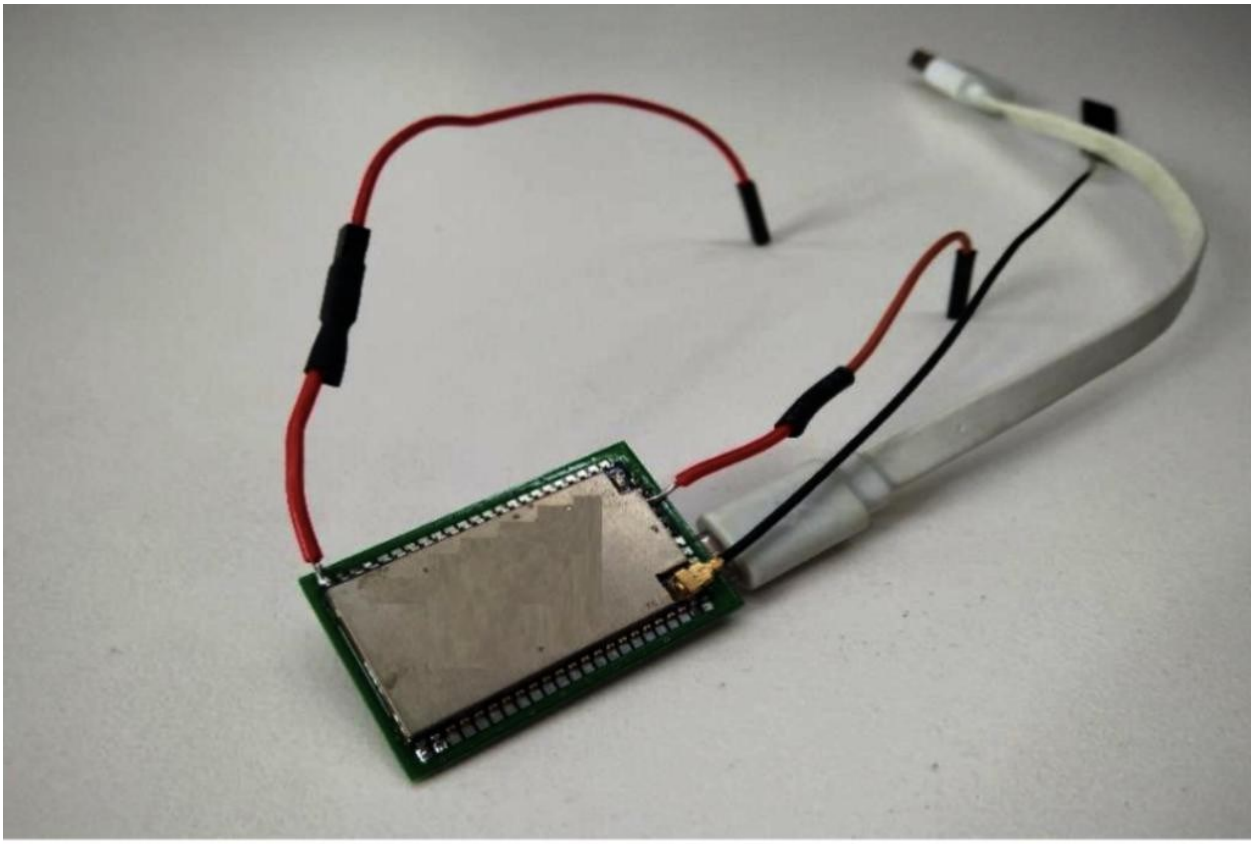
（WiFi 抵近攻击系统（基础版）运行形态图）

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。



（WiFi 抵近攻击系统（mini 版）运行形态图）

Wi-Fi Proximity Attack System (mini version)



（WiFi 抵近攻击系统（mini 版）产品实物图）

Wi-Fi Proximity Attack System (mini version product picture)

4. Conclusion

The revelation of the extensive data breach targeting iSoon, a China-based company associated with the Ministry of Public Security, underscores the sophistication and breadth of Chinese cyber intelligence operations. The disclosed information exposes a wide array of tools and techniques the attackers employ, shedding light on the intricacies of their operational strategies.

In conclusion, this data breach exposes the operational intricacies of Chinese cyber intelligence and raises significant concerns about the potential misuse of advanced cyber tools on a global scale. Addressing these challenges requires the international cybersecurity community's collaborative and proactive approach to mitigate risks, enhance defenses, and safeguard the digital landscape against evolving threats.