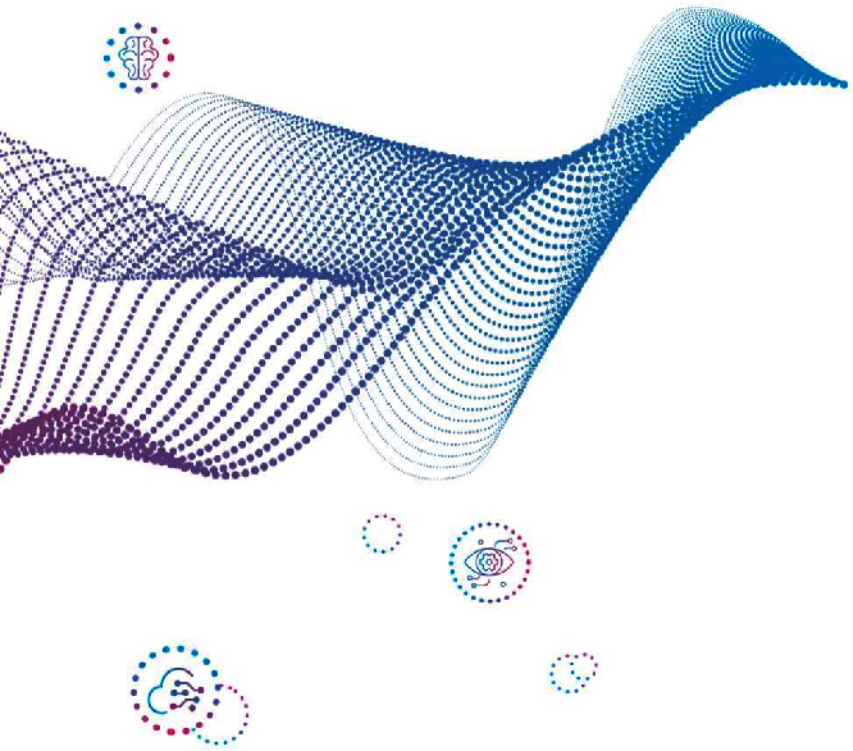
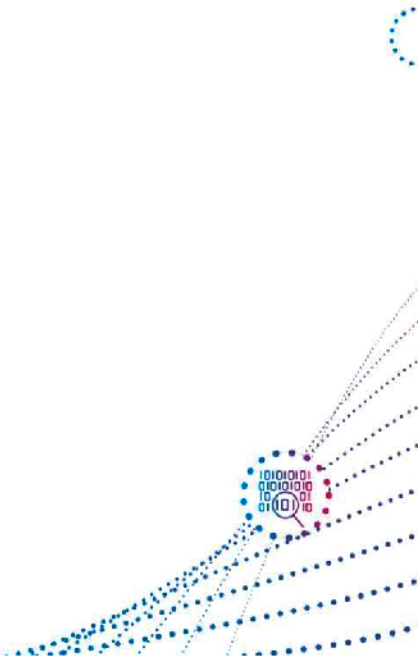



Windows 远程控制管理系统

产品白皮书

(2022 年 V1.0 版本)

目录

1 前言 1

2 需求分析 1

3 产品简介 3

3.1 产品介绍 3

3.2 产品组成 3

3.3 系统架构 4

3.4 网络架构 5

4 产品功能 5

4.1 被控程序生成 6

4.2 远程配置管理 7

4.3 内网级联 7

4.4 资源管理 7

4.5 进程管理 8

4.6 服务管理 9

4.7 注册表管理 9

4.8 CMD 控制台 10

4.9 屏幕截图 10

4.10 键盘记录 11

4.11 文档访问记录 11

4.12 上线日志记录 12

4.13 断开连接 12
4.14 远程卸载 12
4.15 导出报告 13
5 产品参数 13
6 产品部署 14
6.1 适用环境 14
6.2 部署方式 14
7 产品优势 15

1 前言

伴随网络科学技术的飞速发展，计算机的使用已经得到全面的普及。互联网时代的到来，给人们的生活带来了巨大的变化。但是，人们在享受网络技术发展带来的好处的同时，也给犯罪分子提供了更加方便的犯罪环境和工具。以计算机作为通讯载体从事违法犯罪活动日益增多，它们往往会给人们和社会带来不可估量的严重后果和经济损失，甚至威胁到国家安全。中共中央政治局委员、中央政法委书记孟建柱曾指出：网络犯罪已成为第一大犯罪类型，未来绝大多数犯罪都可能借助网络实施。因此，打击利用计算机作为载体进行犯罪的组织，对于人民的利益，社会的发展和国家的稳定有着重大意义。

据统计，2018 年我国网民达到 7.72 亿，其中使用电脑上网的网民中，95%的网民使用 Windows 操作系统。相关业务部门在进行网络 ZC 工作中，必然面对 Windows 系统的 JK 取证，所以，“Windows 远程控制管理系统”的建设符合国家稳定发展的趋势，同时，对打击以 Windows 操作系统为基础的网络犯罪活动具有极其重要的意义。

2 需求分析

为保障“Windows 远程控制管理系统”的建设能够满足建设目标，并且能够在后期的网络实战中提供全方位的技战术支撑，使其具有实战价值和实战意义，因此整套系统的建设应满足隐蔽免杀功能、系统全面覆盖、功能设计丰富的整体建设需求。

(一) 隐蔽免杀功能

“Windows 远程控制管理系统”在进行 ZR 取证的过程当中系统应满足隐蔽免杀的功能需求，系统能够在数据回传时进行链路加密，避免 JK 泄露；同时，需满足避免国内外主流杀毒软件查杀的功能，避免犯罪分子察觉，进行长期 JK 取证。

(二) 系统全面覆盖

基于目前 Windows 操作系统版种类繁多的现状，整套系统应全面覆盖不同类别不同版本的

Windows 操作系统，从而满足在实战应用中能够对各类 Windows 系统进行 ZR 和取证的需求。

(三)　功能设计丰富

在完成针对目标 Windows 系统 ZR 后，能够满足安全、稳定、隐蔽的取证要求，并且结合目标 Windows 系统所处网络环境提供完善的功能应用，能够实现针对目标 Windows 系统的数据获取、远程控制、内网级联等功能需求。

3 产品简介

3.1 产品介绍

由于互联网的高速发展，以及 Windows 操作系统电脑的大量普及，违法犯罪分子通过网络进行联系、策划组织各种违法犯罪活动，给人民带来了巨大得伤害和损失，严重影响了社会和国家得稳定以及发展，而“Windows 远程控制管理系统”可针对目标 Windows 主机进行 JK 取证，极大限度的预防了违法犯罪行为的发生，保证人民人身财产安全，维护社会和国家稳定发展。

基于主流网络架构和 Windows 系统环境自主研发，实现对 Windows 系统的远程操作、JK 和取证。通过将生成器生成的控制程序 ZR 目标主机并运行，技术人员可以在控制端查看目标主机信息，并根据 ZC 人员指令，将目标主机数据返回给 ZC 人员。增加相关业务部门提前掌握信息，提前做好相关防御措施，同时，隐蔽准确掌握违法分子犯罪证据，打击违法犯罪，保障国家和人民生命财产安全。

3.2 产品组成

“Windows 远程控制管理系统”采用 C/S 结构进行架设，系统软件包含生成器和控制器，用户利用生成器，生成控制程序，控制器可管理和使用系统功能，“Windows 远程控制管理系统”产品组成清单主要如下：

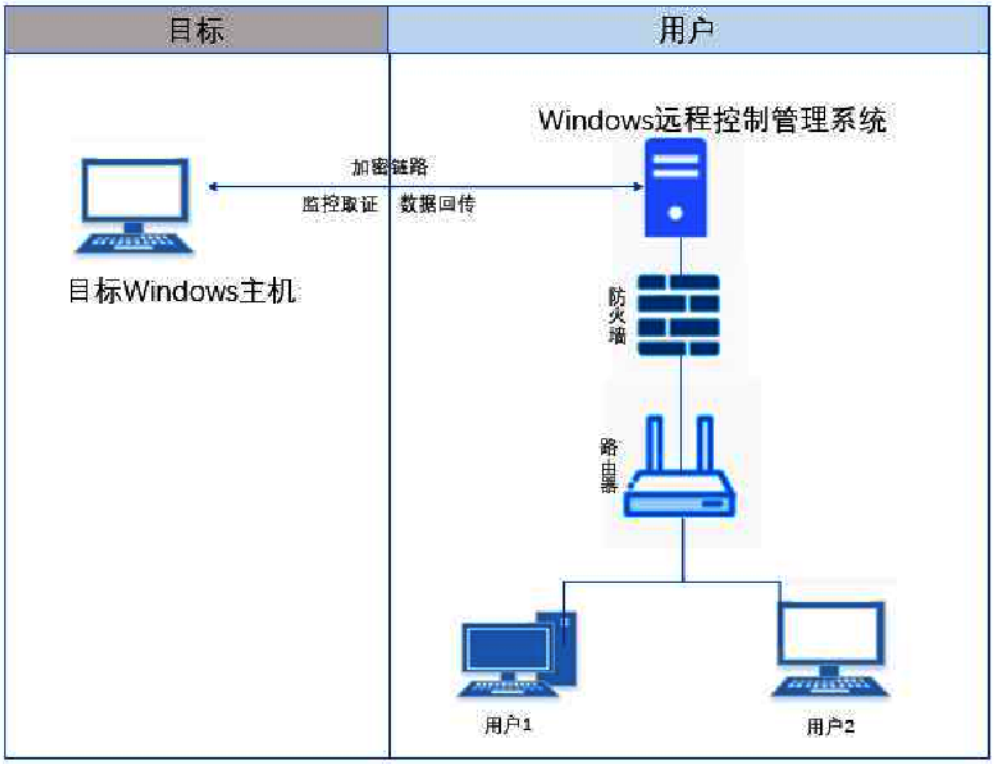
1. “Windows 远程控制管理系统”软件：1 套
2. 产品授权加密狗：1 个
3. 产品使用手册：1 份

3.3 系统架构

（系统架构图）

“Windows 远程控制管理系统”主要由控制器和生成器两个部分组成。用户通过生成器生成控制程序，利用相关手段将程序 ZR 目标主机，达到对目标主机长期隐蔽 JK 取证目的；控制器主要提供用户操作平台，用户可根据自身需求，对目标主机进行资源管理、进程管理、CMD 控制、屏幕截图和键盘记录等操作，并将获取的目标信息进行加密回传。

3.4 网络架构

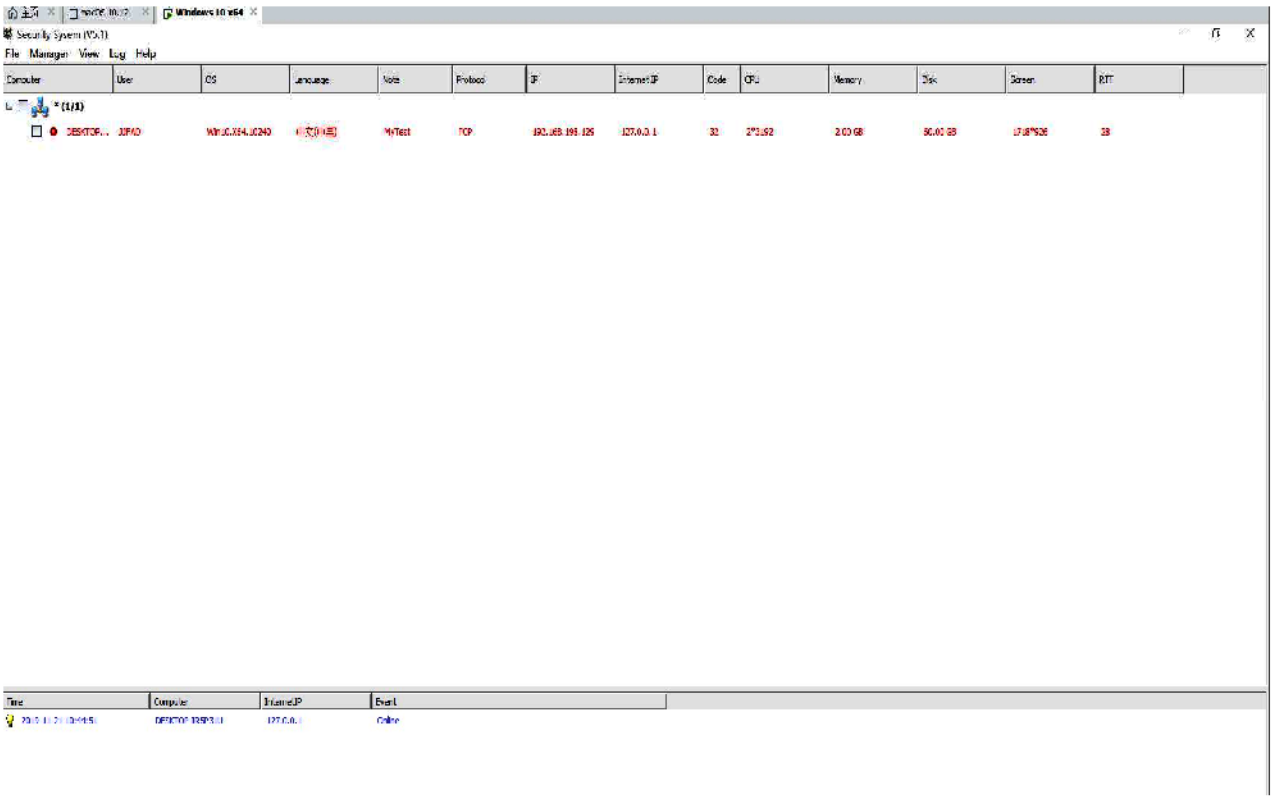


(网络架构图)

平台采用 C/S 架构，满足各种场景下对不同目标 Windows 主机进行远程 JK 管理和取证操作。当目标主机成功被 ZR 控制程序并上线之后，用户只需通过网络便可进入系统后台，对目标 Windows 进行 JK 取证操作。同时，目标数据回传链路采用独有技术进行强加密，保障数据回传过程的安全性，避免被监听的风险存在。

4 产品功能

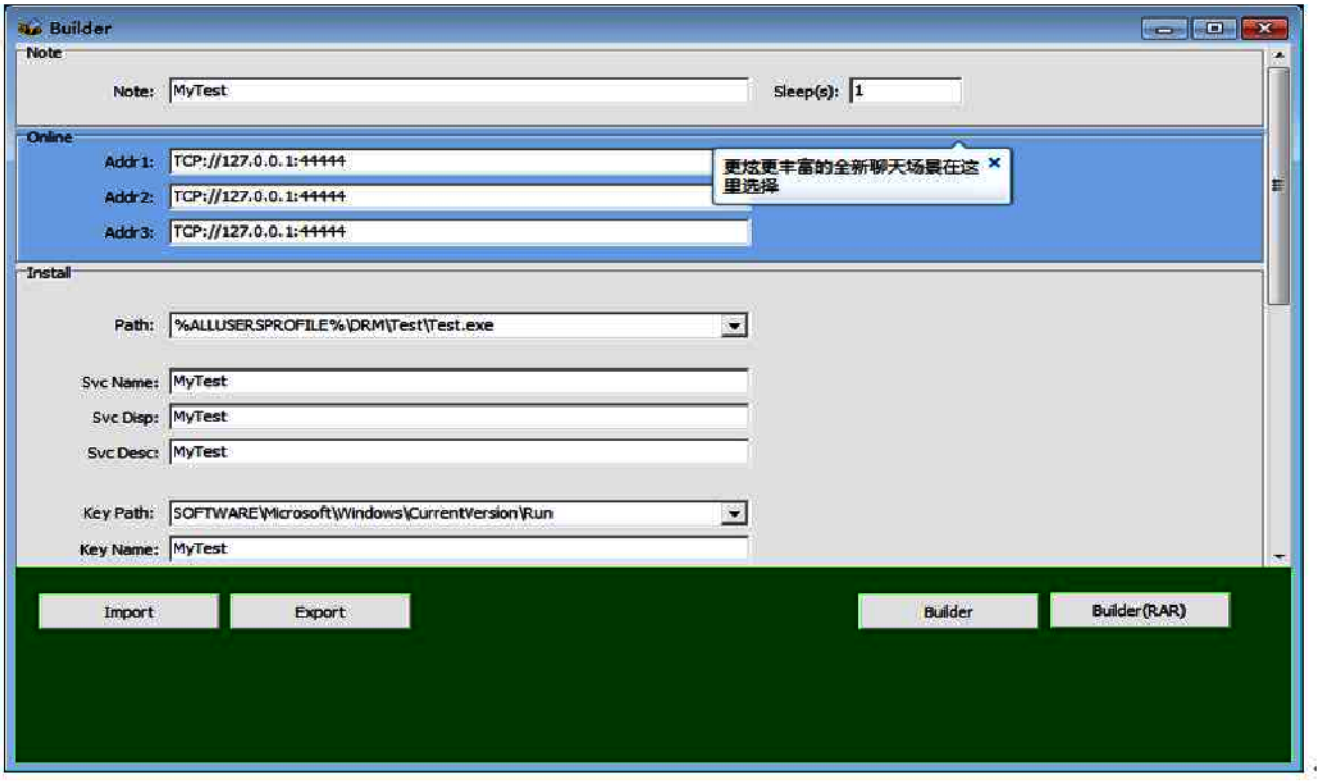
“Windows 远程控制管理系统”结合用户实际需求，设计有资源管理、进程管理、服务管理、注册表管理、CMD 控制台、屏幕截图、键盘记录、文档访问记录、上线日志记录等功能项，充分满足用户对目标 Windows 的长期 JK 和隐蔽取证



（系统功能截图）

4.1 被控程序生成

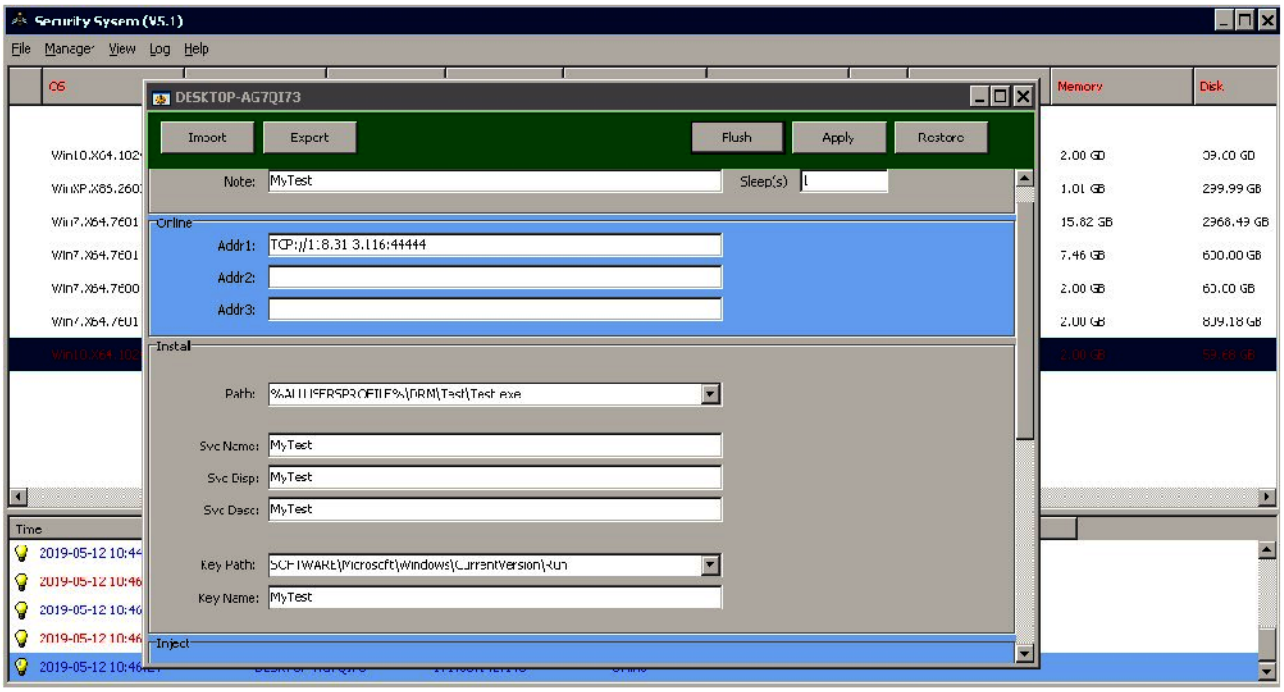
“Windows 远程控制管理系统”的客户端与生成器部署成功后，利用被控程序生成功能可生成控制程序，系统提供键入目标环境对应的 IP 及端口号参数最终生成适应于目标环境的控制程序。



(被控程序生成截图)

4.2 远程配置管理

“Windows 远程控制管理系统”在针对目标 Windows 终端系统 ZR 成功并在后台设备上线成功后，为适应目标应用场景变化的情况，系统提供远程配置管理功能，利用远程配置管理功能系统可再次配置当前被控端 Windows 系统的 IP 及端口号保障系统的长期有效和可靠。



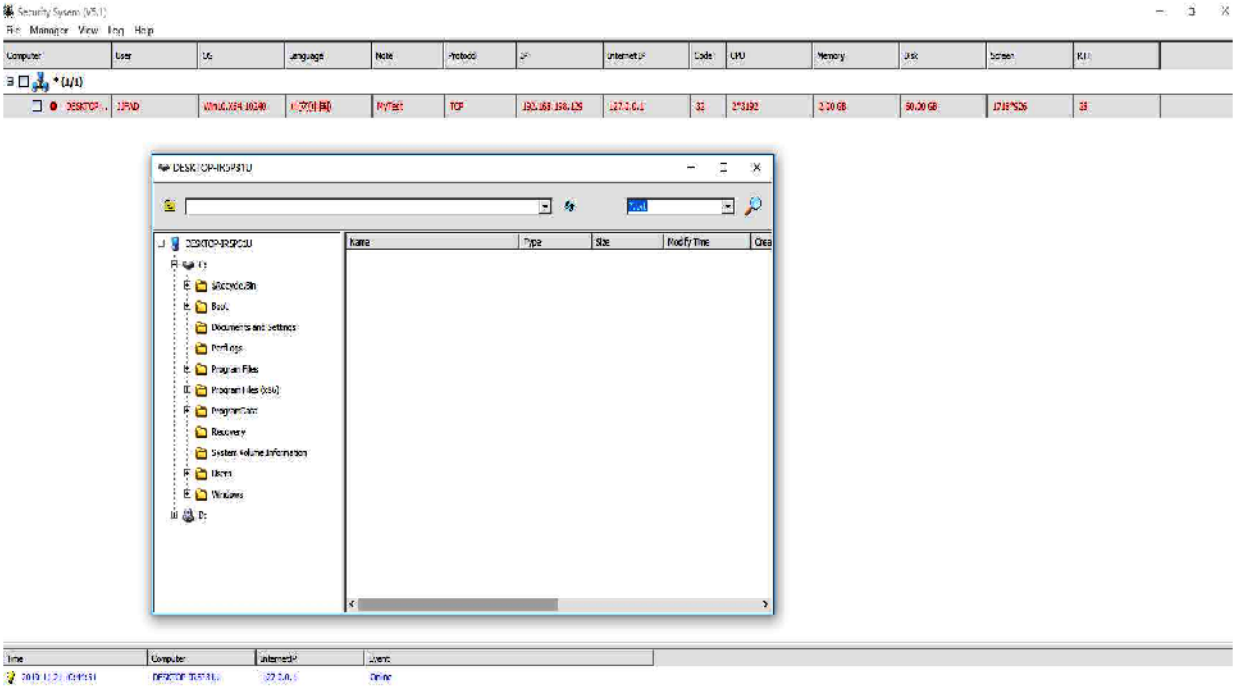
(远程配置管理界面截图)

4.3 内网级联

“Windows 远程控制管理系统”适用于针对内外网隔离的网络环境，当目标内网设备无法访问互联网时，可由同一网域内其他能够访问外网的设备进行级联安装，从而完成对目标内网设备的上线的操作。

4.4 资源管理

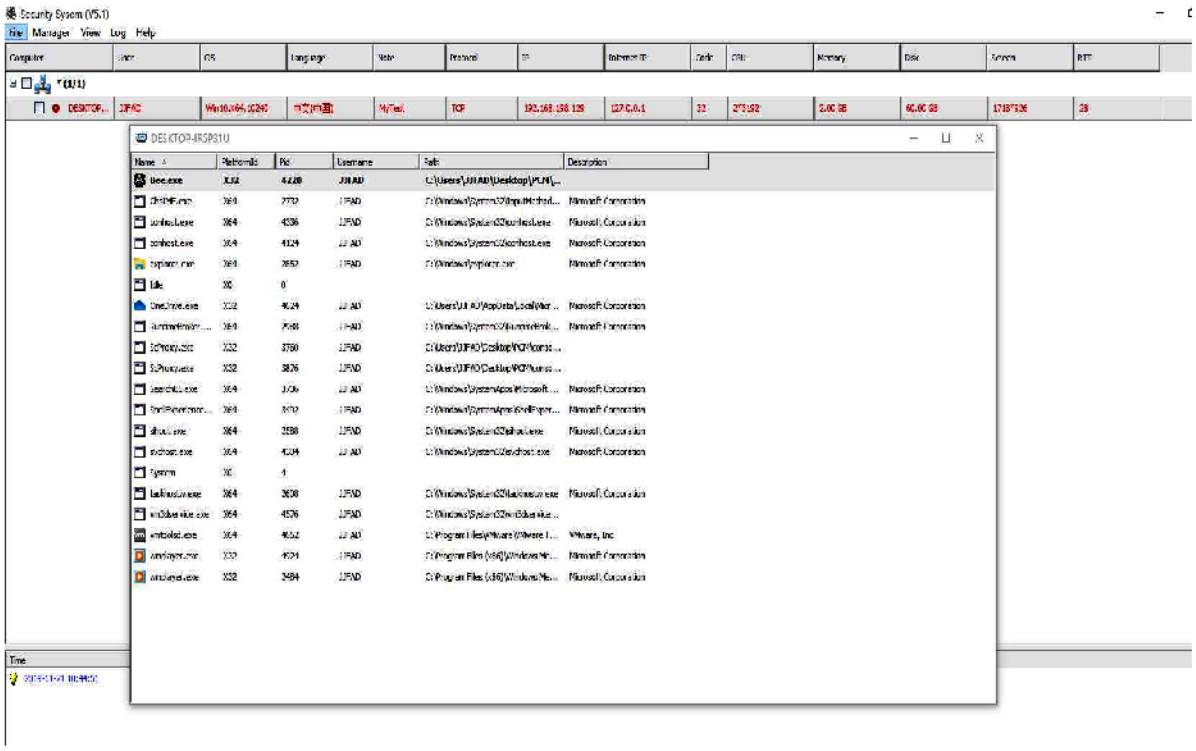
通过对目标主机的程序 ZR，获取目标操作权限，用户可通过系统后台远程操作，对目标操作系统的文件进行综合管理，对相关文件进行浏览操作、上传、下载、删除、执行、重命名等操作。



（资源管理截图）

4.5 进程管理

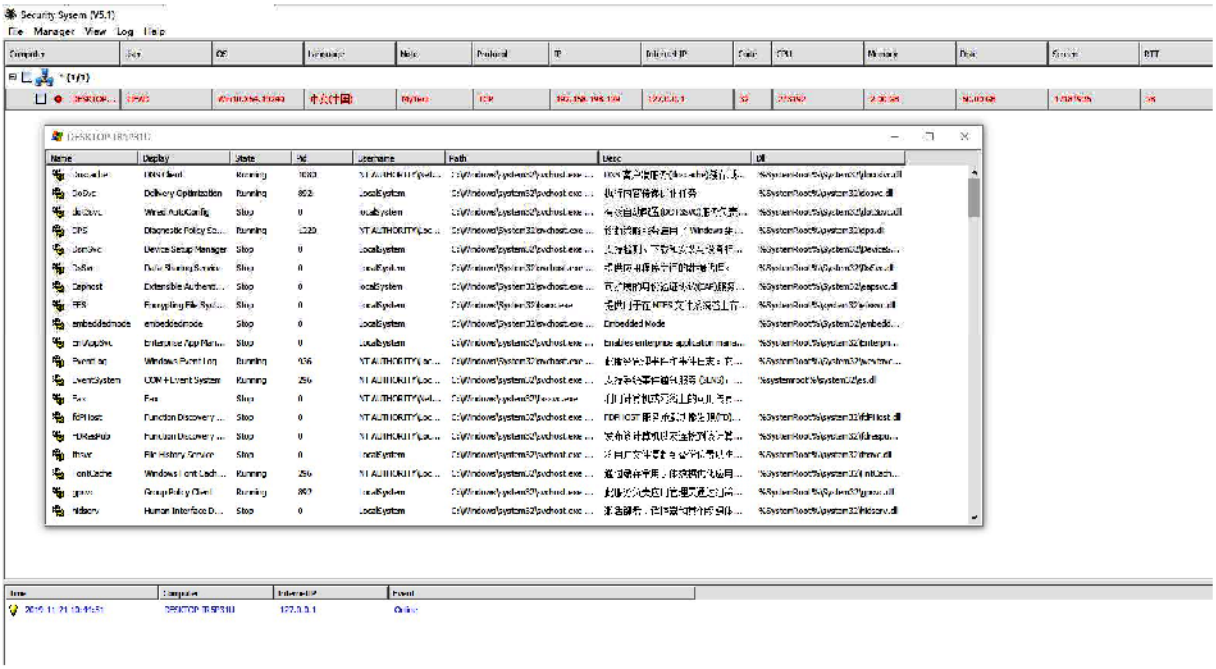
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标操作系统上运行的应用进程、后台进程、Windows 进程等进行实时监督和控制。包括查看刷新、结束等操作。



（进程管理截图）

4.6 服务管理

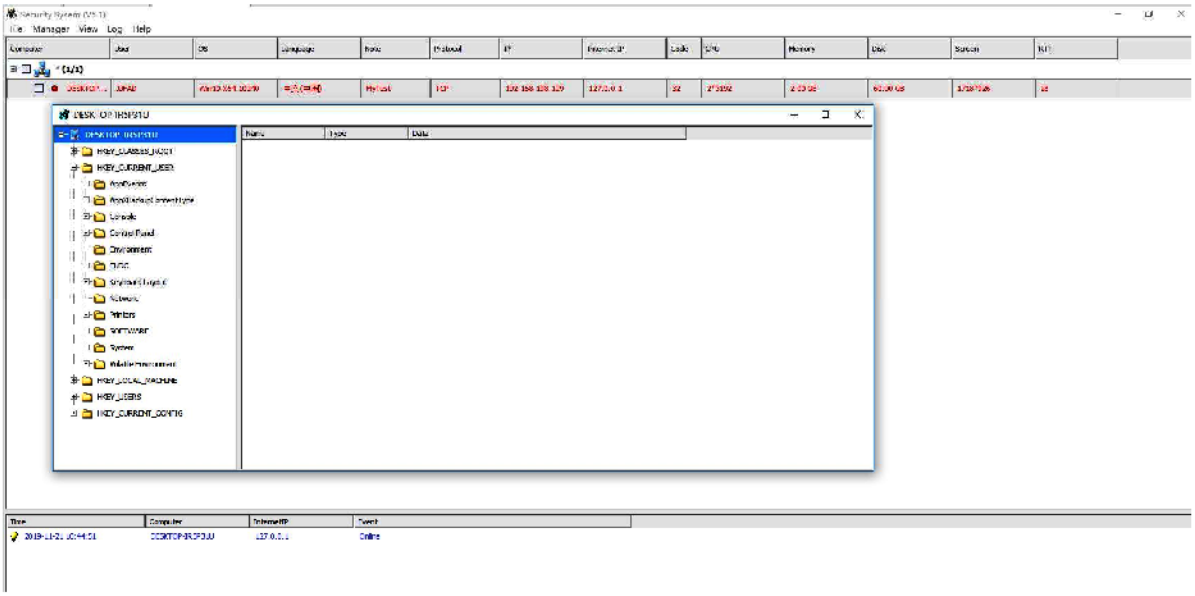
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标操作系统的各项服务状态实时远程管理。包括运行、暂停、停止、删除等操作。



（服务管理截图）

4.7 注册表管理

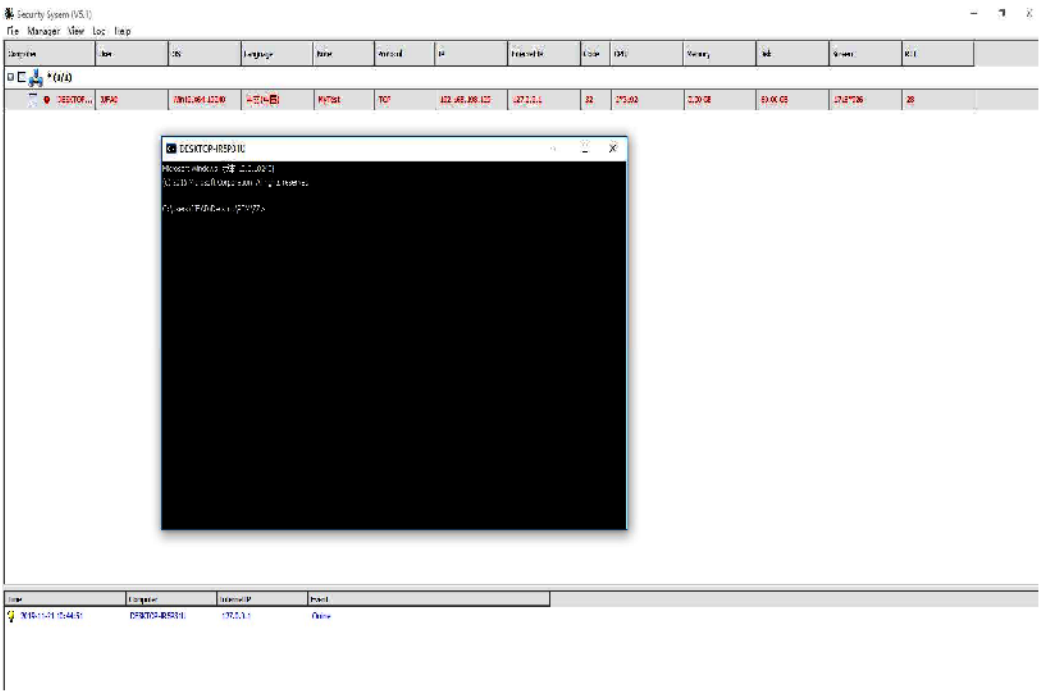
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对操作系统注册表的远程管理。包括查看相关程序的注册表信息、对注册表信息进行修改、删除等操作。



(注册表管理截图)

4.8 CMD 控制台

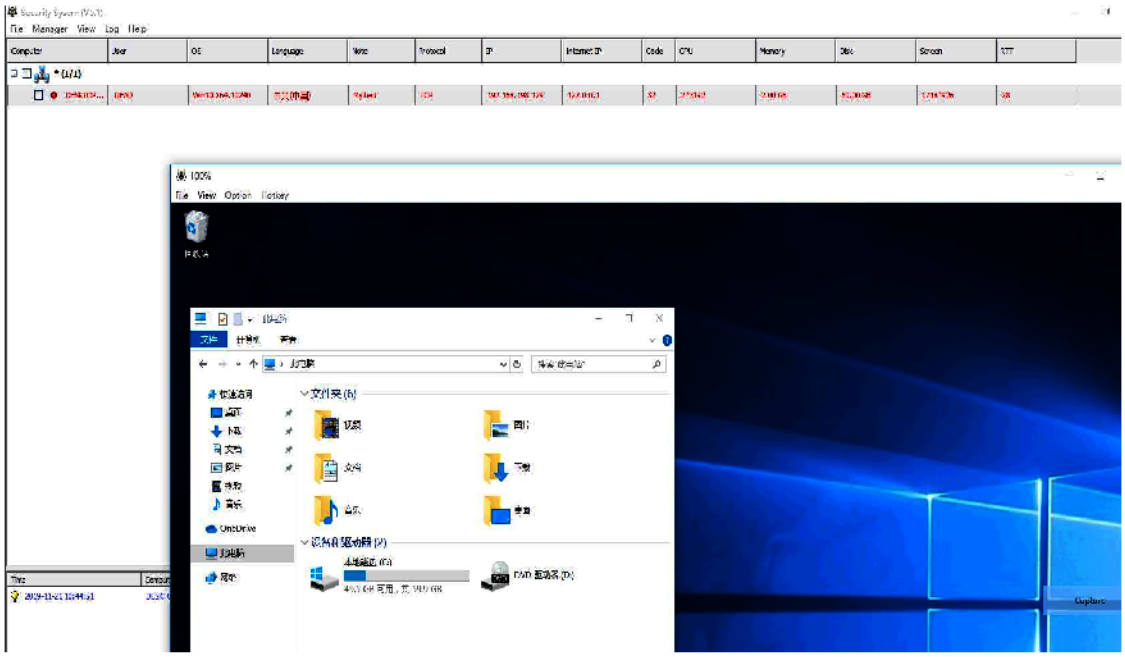
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标操作系统进行 CMD 命令操作。



(CMD 控制台截图)

4.9 屏幕截图

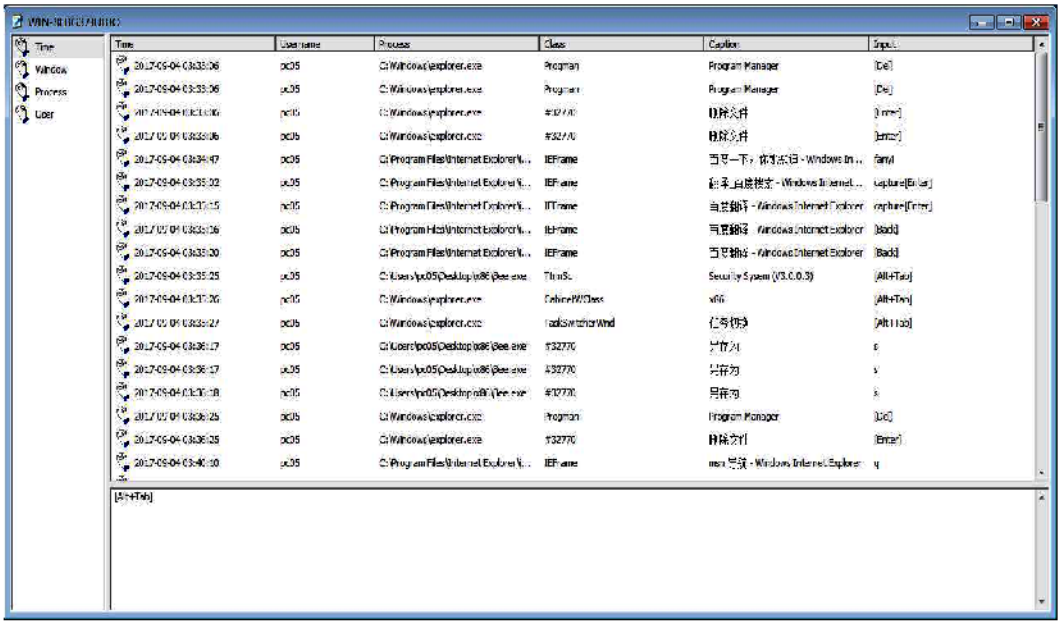
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标操作系统的电脑进行屏幕截图操作。



(屏幕截图)

4.10 键盘记录

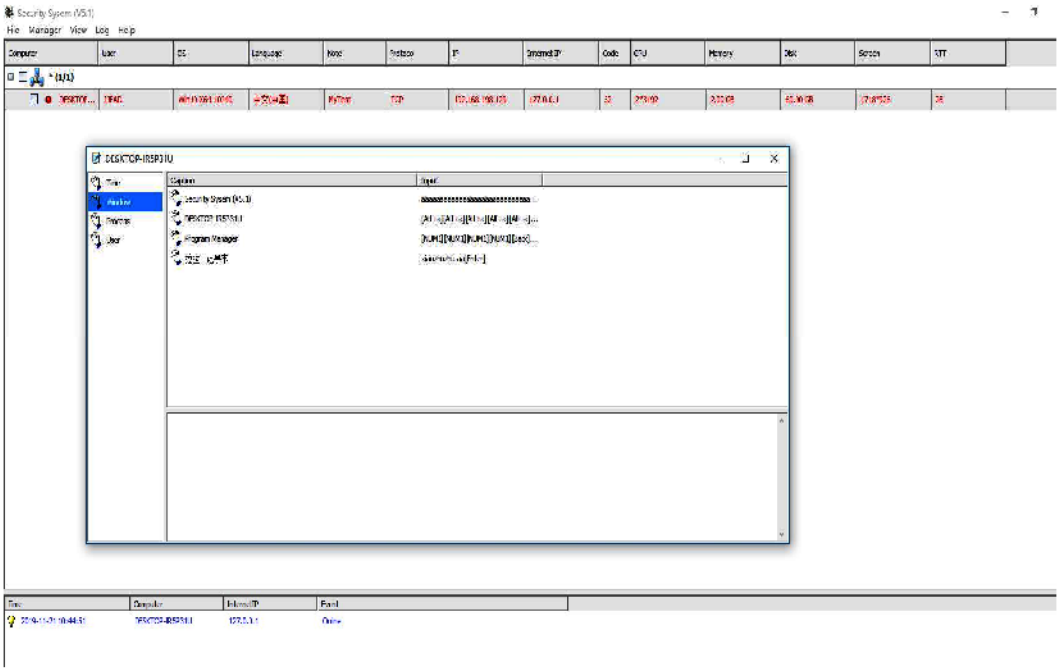
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标操作键盘时按下的每个按键进行记录。



(键盘记录截图)

4.11 文档访问记录

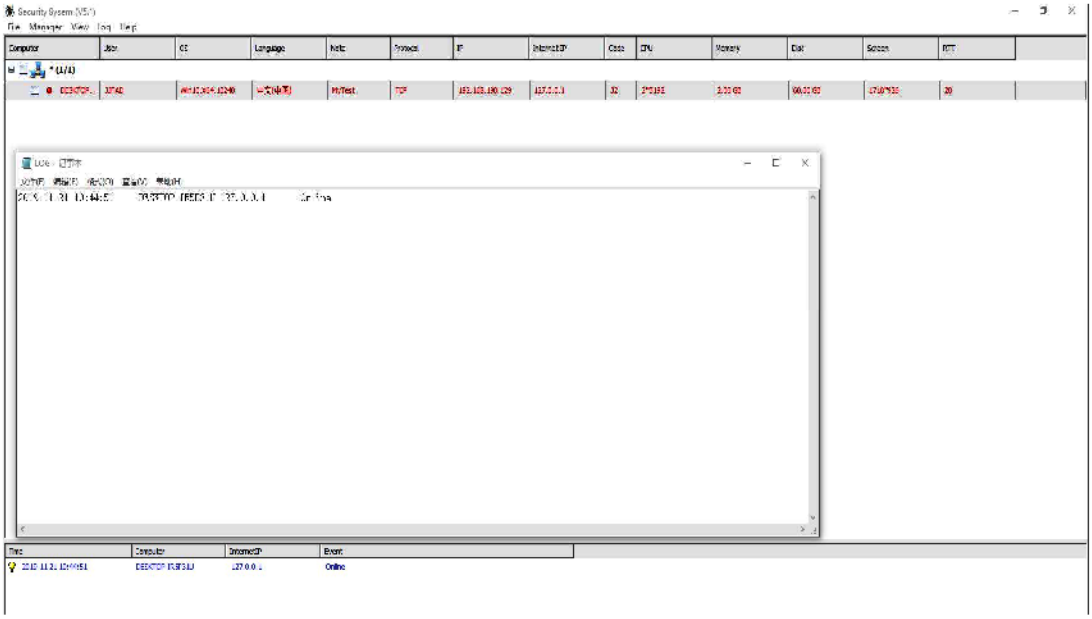
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标最近访问的文件进行记录。可对获取到的文档文件进行查看、修改、删除等操作。



(文档访问记录截图)

4.12 上线日志记录

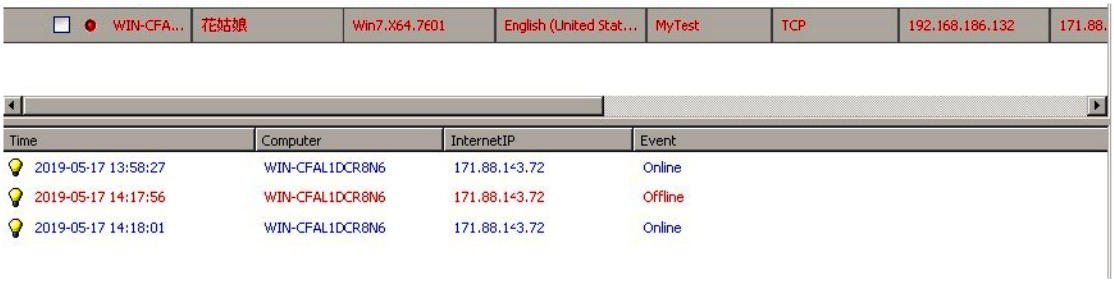
通过对目标主机的程序 ZR，“Windows 远程控制管理系统”支持对目标主机的上线、下线时间等日志进行记录。



（上线日志记录截图）

4.13 断开连接

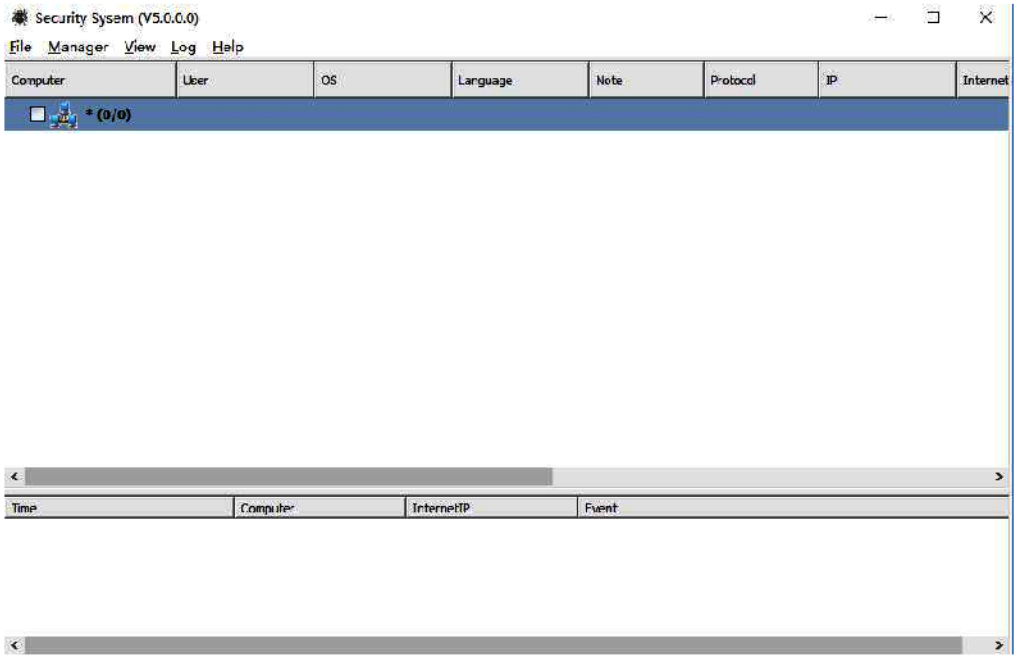
“Windows 远程控制管理系统”具有主动断开连接功能，在主动断开连接后，被控端支持对上线域名 DNS 解析或者上线 IP 地址的实时刷新，支持 TCP、UDP 双协议上线。



（断开连接功能截图）

4.14 远程卸载

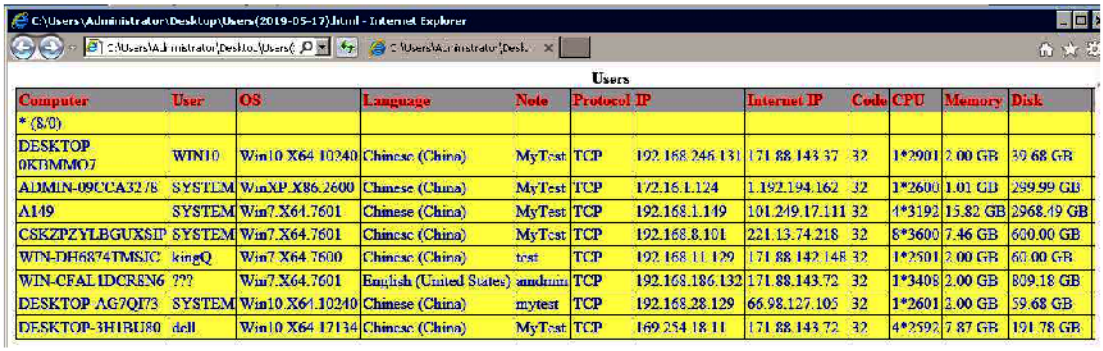
“Windows 远程控制管理系统”具有远程卸载功能，通过对上线设备进行远程卸载操作后。系统会下载所卸载的目标设备信息。



（远程卸载功能截图）

4.15 导出报告

“Windows 远程控制管理系统”具有导出报告功能，系统能够一列表的方式查看目标电脑的用户、系统、语言、上线协议、IP 信息等综合信息。



Users

Computer	User	OS	Language	Note	Protocol	IP	Internet IP	Code	CPU	Memory	Disk
* (8/0)											
DESKTOP 0KBMMO7	WIN10	Win10 X64 10240	Chinese (China)	MyTest	TCP	192.168.246.131	171.88.143.37	32	1*2901	2.00 GB	39.68 GB
ADMIN-09CCA32/8	SYSTEM	WinXP X86 2600	Chinese (China)	MyTest	TCP	172.16.1.124	1.192.194.162	32	1*2600	1.01 GB	299.99 GB
A149	SYSTEM	Win7 X64 7601	Chinese (China)	MyTest	TCP	192.168.1.149	101.249.17.111	32	4*3192	15.82 GB	2968.49 GB
CSKZPZYLBGUXSIP	SYSTEM	Win7 X64 7601	Chinese (China)	MyTest	TCP	192.168.8.101	221.13.74.218	32	8*3600	7.46 GB	600.00 GB
WIN-DH6874TMSIC	kingQ	Win7 X64 7600	Chinese (China)	test	TCP	192.168.11.129	171.88.142.148	32	1*2501	2.00 GB	60.00 GB
WIN-CFALIDCR8N6	???	Win7 X64 7601	English (United States)	anadmin	TCP	192.168.186.132	171.88.143.72	32	1*3408	2.00 GB	809.18 GB
DESKTOP AG7QI73	SYSTEM	Win10 X64 10240	Chinese (China)	mytest	TCP	192.168.28.129	66.98.127.105	32	1*2601	2.00 GB	59.68 GB
DESKTOP-3HIBU80	dell	Win10 X64 17134	Chinese (China)	MyTest	TCP	169.254.18.11	171.88.143.72	32	4*2592	7.87 GB	191.78 GB

（导出报告功能截图）

5 产品参数

类别	参数
架构	C/S 架构
ZR 方式	系统生成器生成 exe 可执行文件安装
适配系统	Windows XP/Vista/7/8/8.1/10

	Windows Server 2003/2008/2012/2016
上线方式	TCP/UDP/网络互联协议
上线时间	1 分钟以内
数据获取	支持
日志管理	支持
防病毒免杀	支持
内网级联	支持

6 产品部署

6.1 适用环境

“Windows 远程控制管理系统”针对非法犯罪份子的终端电脑进行程序 ZR，从而实现对目标犯罪份子进行犯罪取证的场景，在 ZR 目标 PC 成功后，通过授权加密狗就可直接登录后台管理平台，即可对目标 PC 进行数据信息获取，为确保整个系统的稳定运行，“Windows 远程控制管理系统”被控端适用环境要求如下：

程序	操作系统位数	操作系统版本
被控端(客户端)	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
控制端	X64/86	Windows XP/Vista/7/8/8.1/10 Windows Server 2003/2008/2012/2016

6.2 部署方式

“Windows 远程控制管理系统”采 C/S 架构进行部署，部署方便快捷，系统只需提供一套

VPS 服务器便可搭载后台管理系统，利用授权加密狗和账号登录到系统后台，即可使用生成器进行 ZR 程序的生成，ZR 成功后，后台即可上线目标设备信息，获取目标设备数据信息。VPS 配置如下：

配置环境	环境参数
VPS 服务器配置要求	CPU：双核
	内存：4G
	硬盘：100G
	系统：Windows server
	带宽：≥10Mbps

7 产品优势

- **稳定性高**

整套系统基于远程控制新趋势，结合当前主流网络架构和 Windows 系统环境自主研发，采用独立代码进行维护、独立密钥认证、独立自主加密算法进行加密传输，在确保系统功能的情况下，充分保障了系统具有高稳定性且不易掉线。

- **传输高效**

系统为实现目标数据高效回传，内置独立下载引擎，可实现文件极限传输，根据网络速度自适应传输文件，在 2M 网络宽带下文件传输速度最高可达 800KB/S.

- **免杀性强**

系统采用业内独有的突破杀软主动防御技术，免杀能力强，能够躲避市面上 95%杀毒软件的查杀，如国内 360、金山杀毒、腾讯电脑管家；国外卡巴斯基、赛门铁克、麦咖啡等主流杀毒软件。并且基于内存多变形制作和文件多态制作双重技术，可有效躲避内存动态扫描和文件静态扫描防护机制。

- **隐蔽性强**

系统支持被控端程序安装后自启动、自删除，并且支持相关程序安装成功后，自动删除安装文件，杜绝被目标发现的可能性。

- **简洁易用**

整个系统应用广泛，支持主流 X86/X64 Windows 操作系统（包括最新的 Win10 系统），系统界面简洁，用户根据自身需要，调用相应功能即可实现，操作简单，非常容易上手。