3 Product Introduction

3.1 Product introduction

Outlook mailbox is a free, web-based email portal service owned by Microsoft. When users log in to Hotmail, they will also be redirected to Outlook mailbox. It is a frequently used enterprise email service brand.

The Microsoft mailbox secret extraction platform has been comprehensively developed and designed based on years of research on the Outlook mailbox login mechanism. By obtaining the target email conversation, it can obtain the target person's email content and grasp key evidence, thereby achieving the purpose of preventing and combating crime.

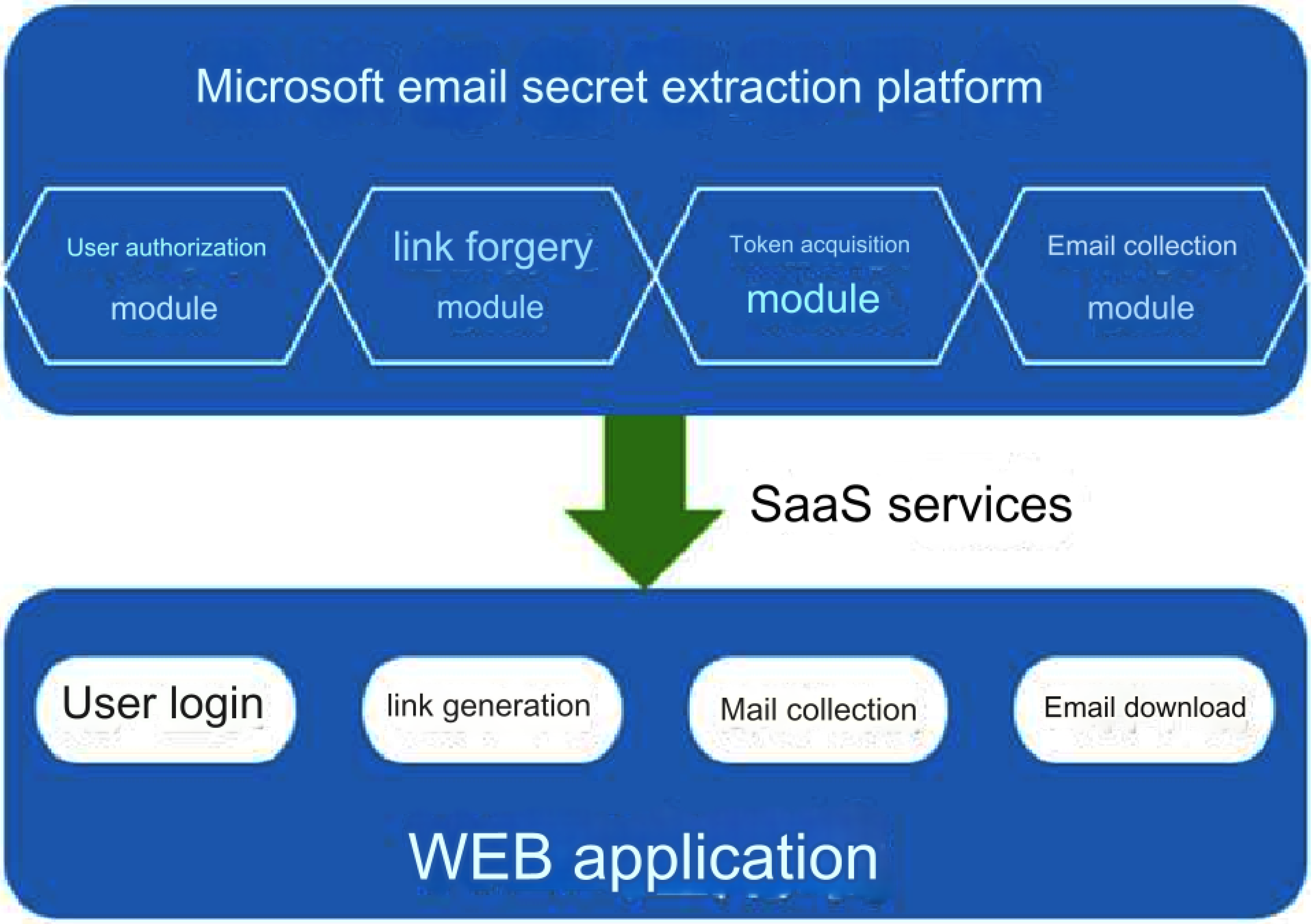
3.2 Product composition

The Microsoft Email Encryption Platform adopts a B/S architecture. Users can log in and use it by specifying an authorized account. The main product components of the Microsoft Email Encryption Platform are as follows:

1. Microsoft email encryption platform account password: 1 set

2. Microsoft email secret extraction platform information: 1 set

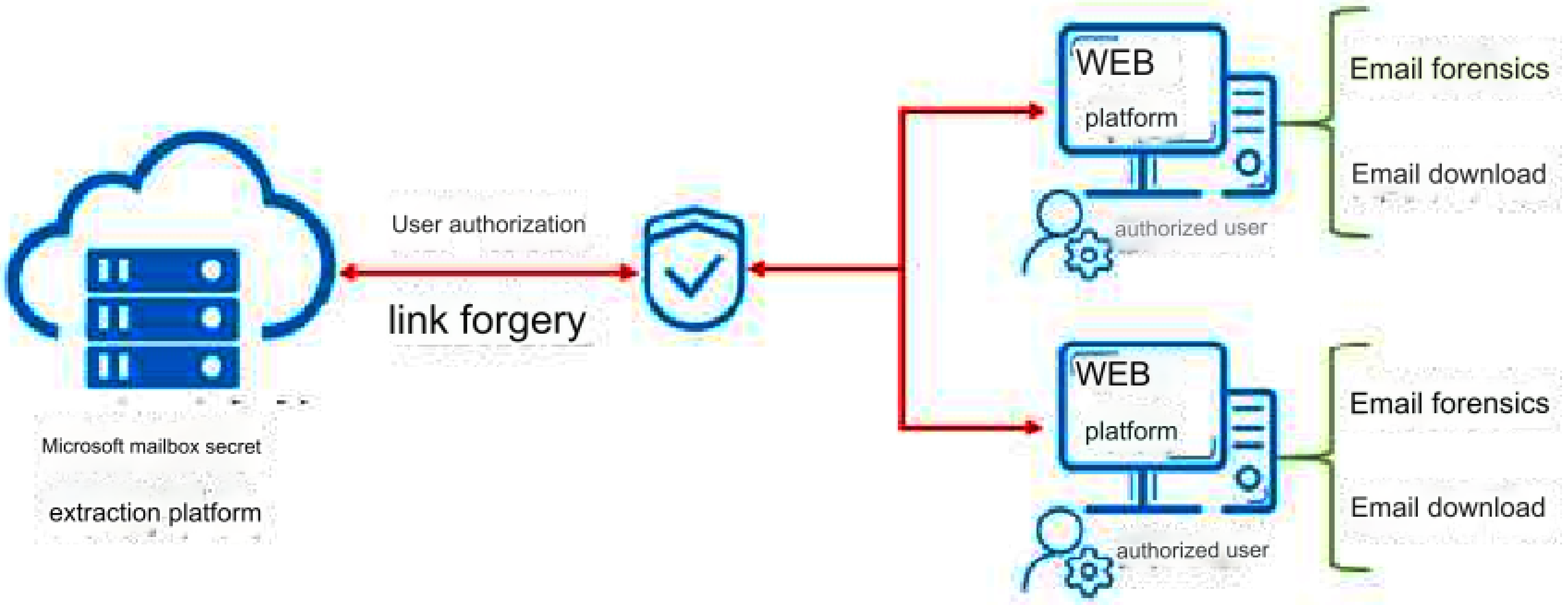
3.3 System architecture



(system architecture diagram)

The Microsoft mailbox encryption platform is mainly used as a SaaS service provided by Anxun Information. The cloud platform is mainly composed of a user authorization module, a link forgery module, a token acquisition module and an email collection module. After purchasing the Microsoft email encryption platform, users obtain corresponding authorized accounts and client application platforms for installation and deployment. Through authorized accounts, users can perform functional operations such as login, link generation, email collection, and email downloading.

3.4 Network architecture



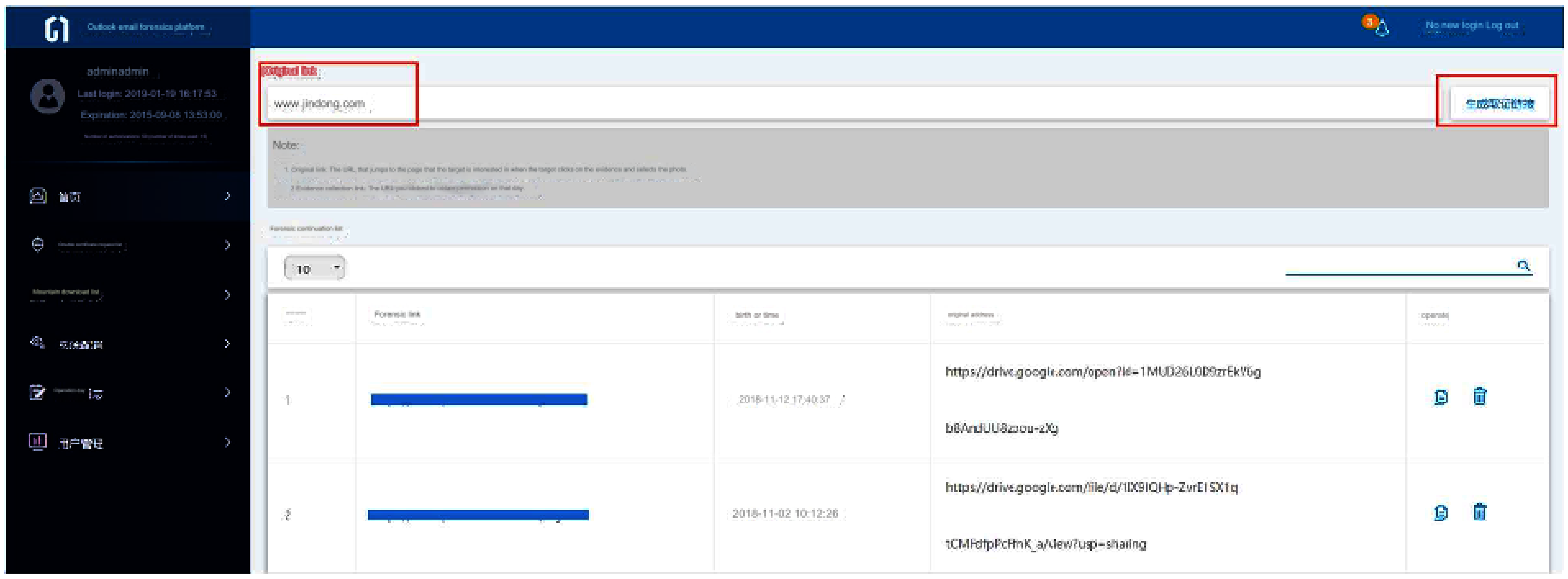
(Network architecture diagram)

The Microsoft mailbox secret extraction platform is mainly constructed and maintained by Anxun Information to ensure the security and stability of the entire system. Users only need to obtain an authorized account and build a WEB client platform, and then they can log in to the WEB application platform through the authorized account. Implement forensic operations on the target Outlook mailbox.

4 product features

4.1 Generate phishing links

Go to the home page, enter the original address in the original link box (the original link is the URL that jumps to the page that the forensic target is interested in after clicking on the forensic link), and click "Generate forensic link", as shown in the figure below:


Outlook email forensics platform
No new login Log out
adminadmin
Last login: 2019-01-19 16:17:53
Expiration: 2015-09-08 13:53:00
首页
Maintain download list
用户管理
Original link
生成取证链接

www.jindong.com

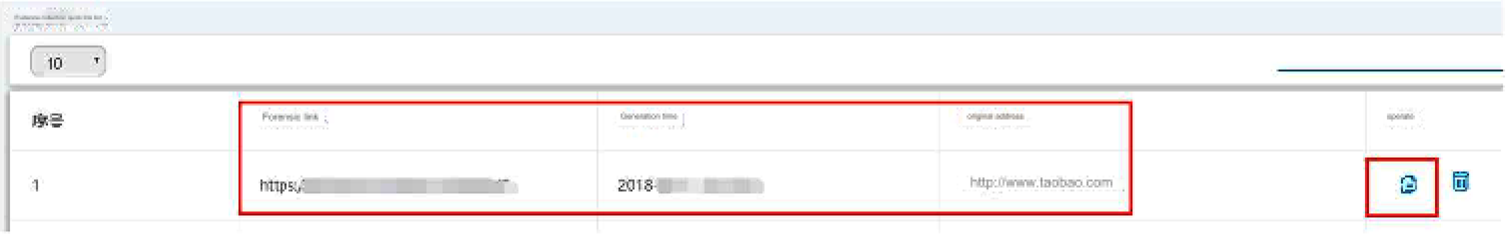
Note:

1. Original link: The URL that jumps to the page that the target is interested in when the target clicks on the evidence and selects the photo.
2 Evidence collection link: The URL you clicked to obtain permission on that day.

Forensic continuation list

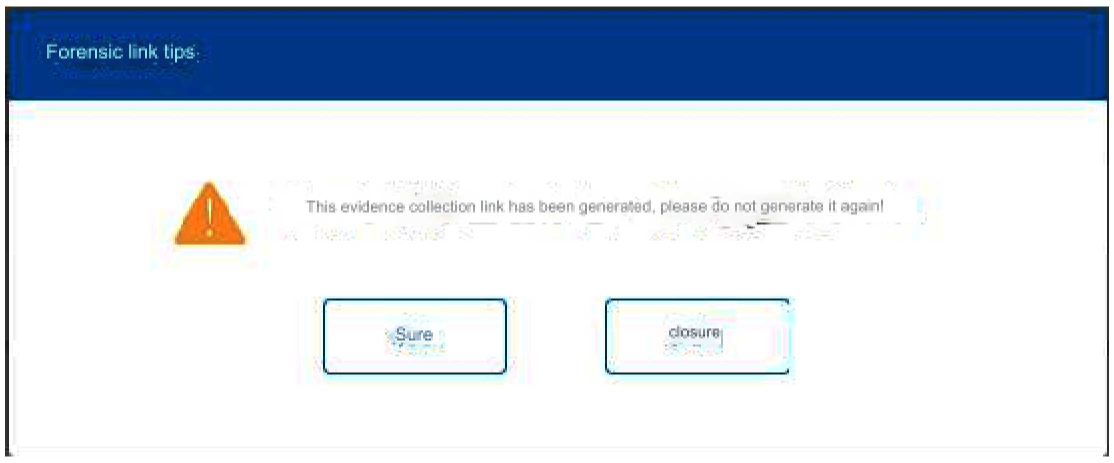
	Forensic link	birth or time	original address	operate
1	[redacted]	2018-11-12 17:40:37	https://drive.google.com/open?id=1MUD26L0D9zrEkV6g bBAndUU8zaou-zXg	
2	[redacted]	2018-11-02 10:12:26	https://drive.google.com/file/d/1lX9IQHp-ZvrE1SX1q tCMHdfpPcHnK_a/view?usp=sharing	

After generation, you will see the generated forensic-link in the latest forensic link list (the URL that the user deceives the target to click to obtain its permissions). Click the copy button in the operation to copy the forensic link, as shown in the figure below:



序号	Forensic link	Generation time	original address	operate
1	https:/[redacted]	2018-[redacted]	http://www.taobao.com	

When the original link of the generated forensic link is the same in the forensic link list, the platform will prompt that the generation failed. In this case, you need to use other original links or delete the generated forensic link, as shown in the following figure:



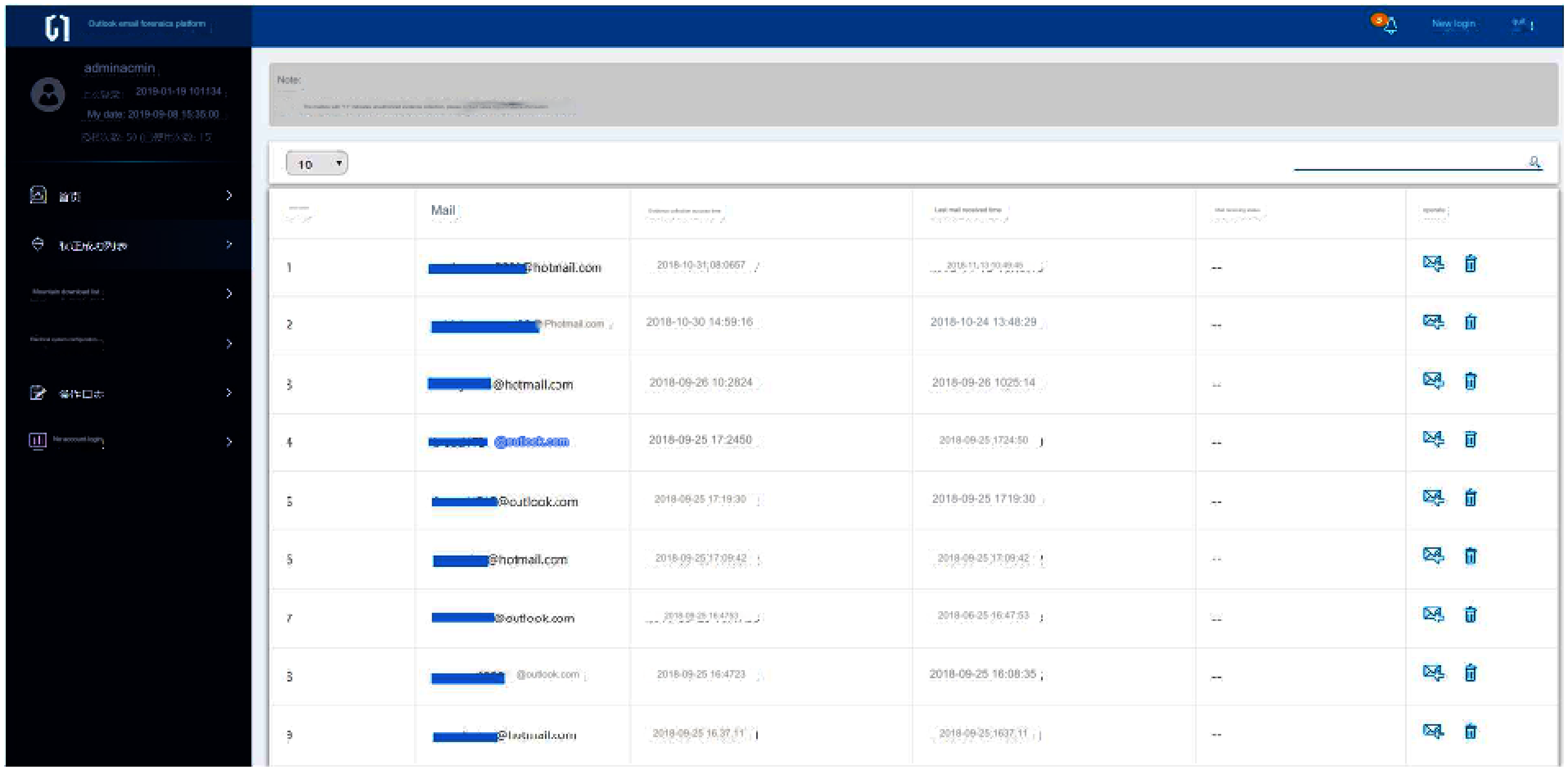
Forensic link tips

This evidence collection link has been generated, please do not generate it again!

4.2 Obtaining emails from the target mailbox

When the target clicks on the evidence collection link, he or she can find the second pass of the non-sense bypass in the "Forensic Success List" of the Microsoft Email Encryption Platform.

Verify and collect all target email data, as shown in the figure below:

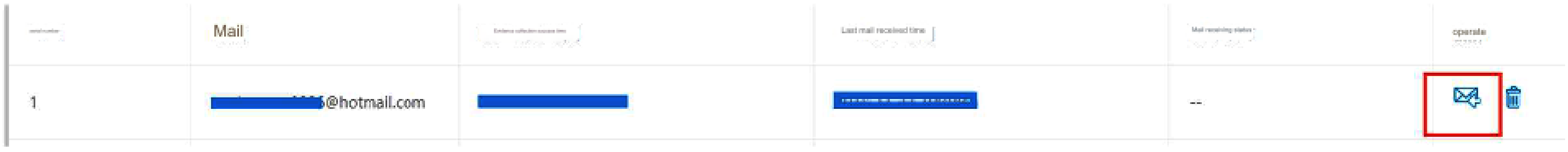


Outlook email forensics platform
New login
adminacmin
2019-01-19 101134
My date: 2019-09-08 15:35:00
Note:
10

[illegible]	Mail	Evidence collection success time	Last mail received time	Mail receiving status	operate
1	[redacted]@hotmail.com	2018-10-31 08:0657	2018-11-13 10:49:46	--	✉ 🗑
2	[redacted]@hotmail.com	2018-10-30 14:59:16	2018-10-24 13:48:29	--	✉ 🗑
3	[redacted]@hotmail.com	2018-09-26 10:2824	2018-09-26 1025:14	--	✉ 🗑
4	[redacted] @outlook.com	2018-09-25 17:2450	2018-09-25 1724:50	--	✉ 🗑
5	[redacted]@outlook.com	2018-09-25 17:19:30	2018-09-25 1719:30	--	✉ 🗑
6	[redacted]@hotmail.com	2018-09-25 17:09:42	2018-09-25 17:09:42	--	✉ 🗑
7	[redacted]@outlook.com	2018-09-25 16:4733	2018-06-25 16:47:53	--	✉ 🗑
8	[redacted] @outlook.com	2018-09-25 16:4723	2018-09-25 16:08:35	--	✉ 🗑
9	[redacted]@hotmail.com	2018-09-25 16:37:11	2018-09-25 1637:11	--	✉ 🗑

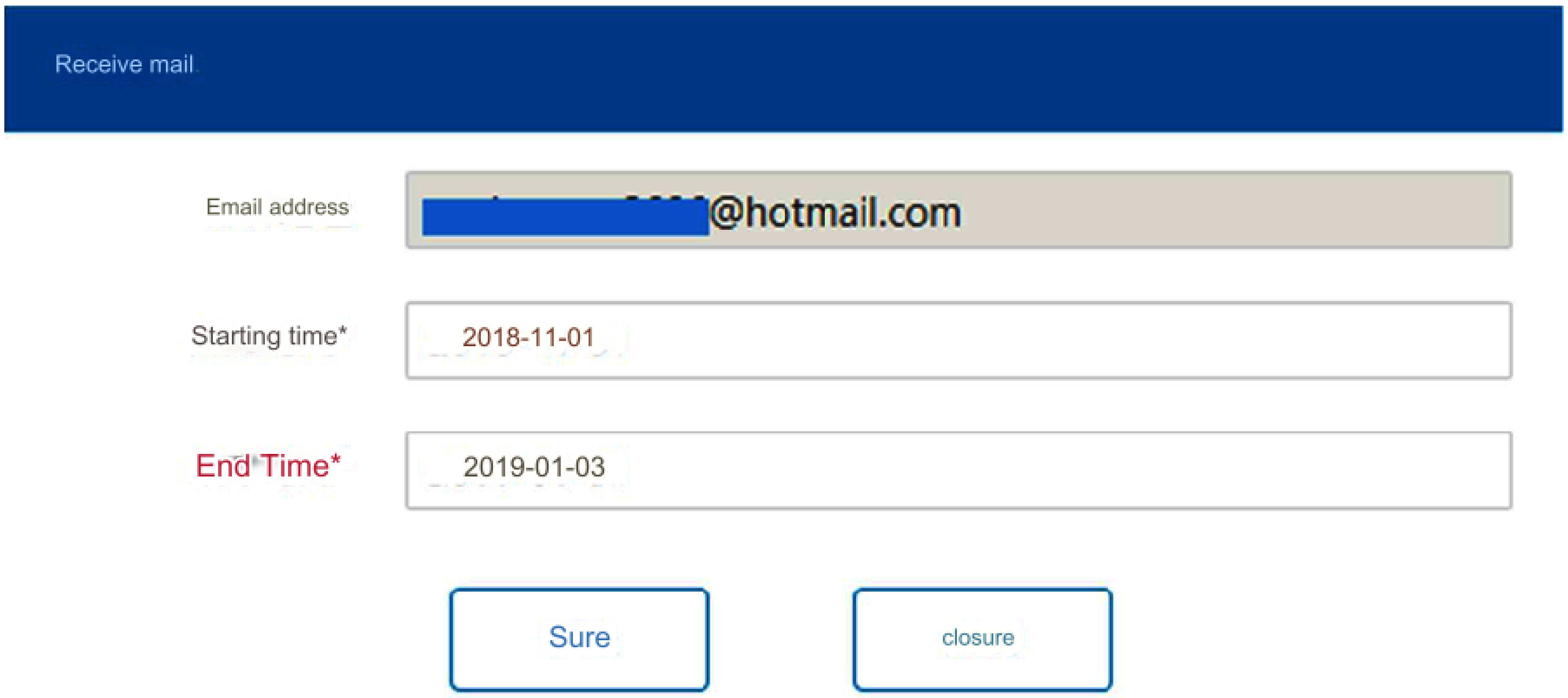
Select the Outlook account you want to receive emails from and click the Receive Mail button in the operation to receive all emails from the target mailbox by date.

Email, as shown below:



[illegible]	Mail	Evidence collection success time	Last mail received time	Mail receiving status	operate
1	[redacted]@hotmail.com	[redacted]	[redacted]	--	✉ 🗑

Select the date of the email you want to receive and click OK, as shown in the figure below:



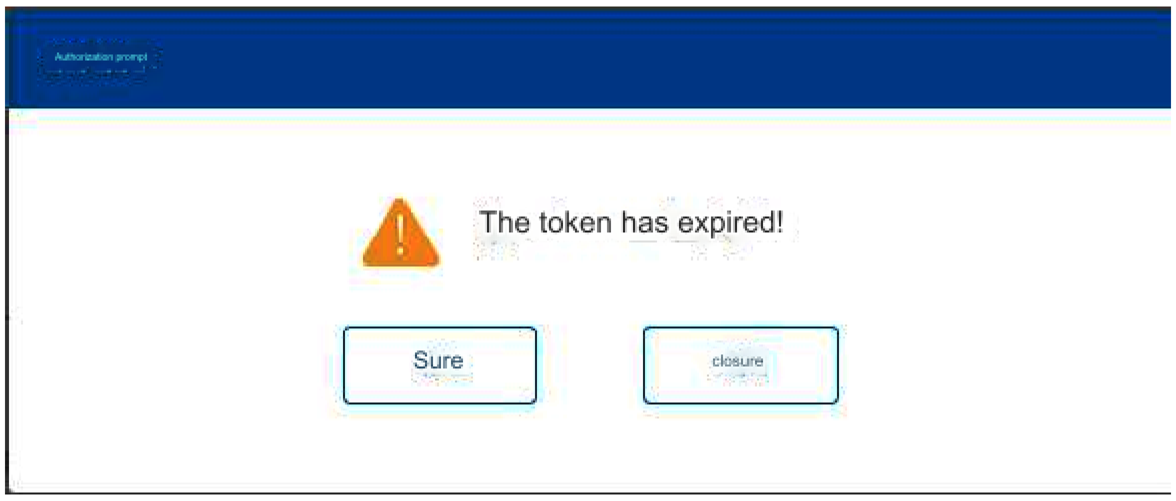
Receive mail

Email address [redacted]@hotmail.com

Starting time* 2018-11-01

End Time* 2019-01-03

As long as the password of the target mailbox has not been changed, the Microsoft mailbox encryption platform can continue to receive emails. If the target changes the login password, the evidence collection link needs to be resent for evidence collection, as shown in the figure below:

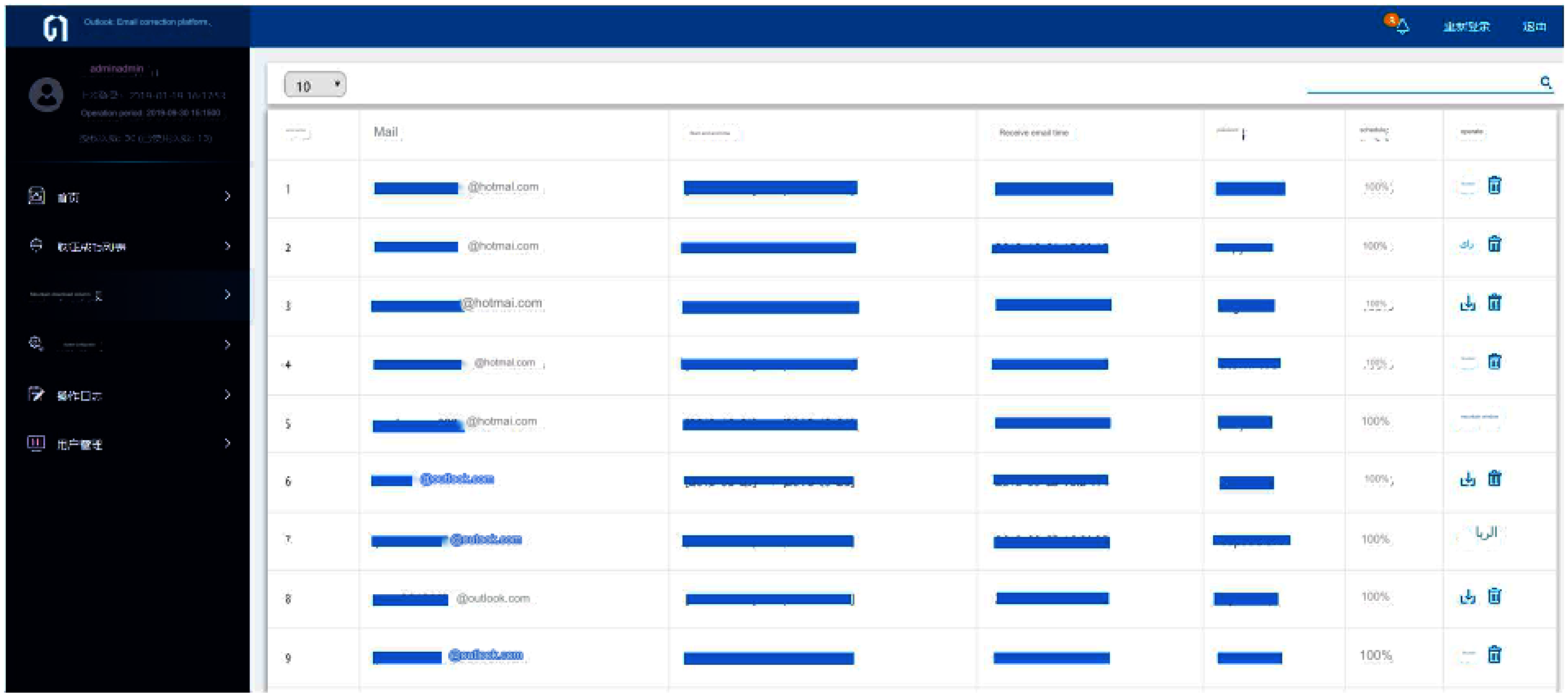


Authorization prompt

The token has expired!

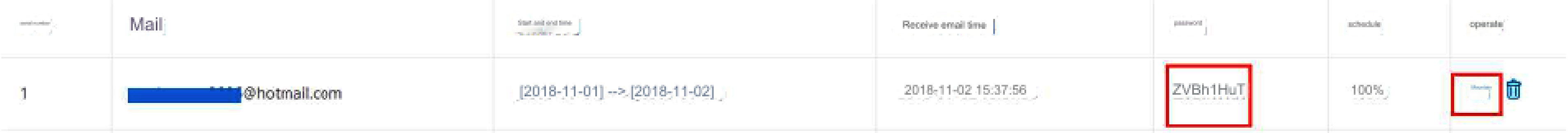
4.3 Email download

Step 1: After successfully obtaining the target mailbox, you can see the progress of obtaining the target mail in the "Download List" of the Microsoft mailbox encryption platform, and download the mail, as shown in the figure below:



[illegible]	Mail	[illegible]	Receive email time	[illegible]	schedule	operate
1	[redacted]@hotmal.com	[redacted]	[redacted]	[redacted]	100%	
2	[redacted]@hotmal.com	[redacted]	[redacted]	[redacted]	100%	
3	[redacted]@hotmail.com	[redacted]	[redacted]	[redacted]	100%	
4	[redacted]@hotmal.com	[redacted]	[redacted]	[redacted]	100%	
5	[redacted]@hotmail.com	[redacted]	[redacted]	[redacted]	100%	
6	[redacted]@outlook.com	[redacted]	[redacted]	[redacted]	100%	
7	[redacted]@outlook.com	[redacted]	[redacted]	[redacted]	100%	
8	[redacted]@outlook.com	[redacted]	[redacted]	[redacted]	100%	
9	[redacted]@outlook.com	[redacted]	[redacted]	[redacted]	100%	

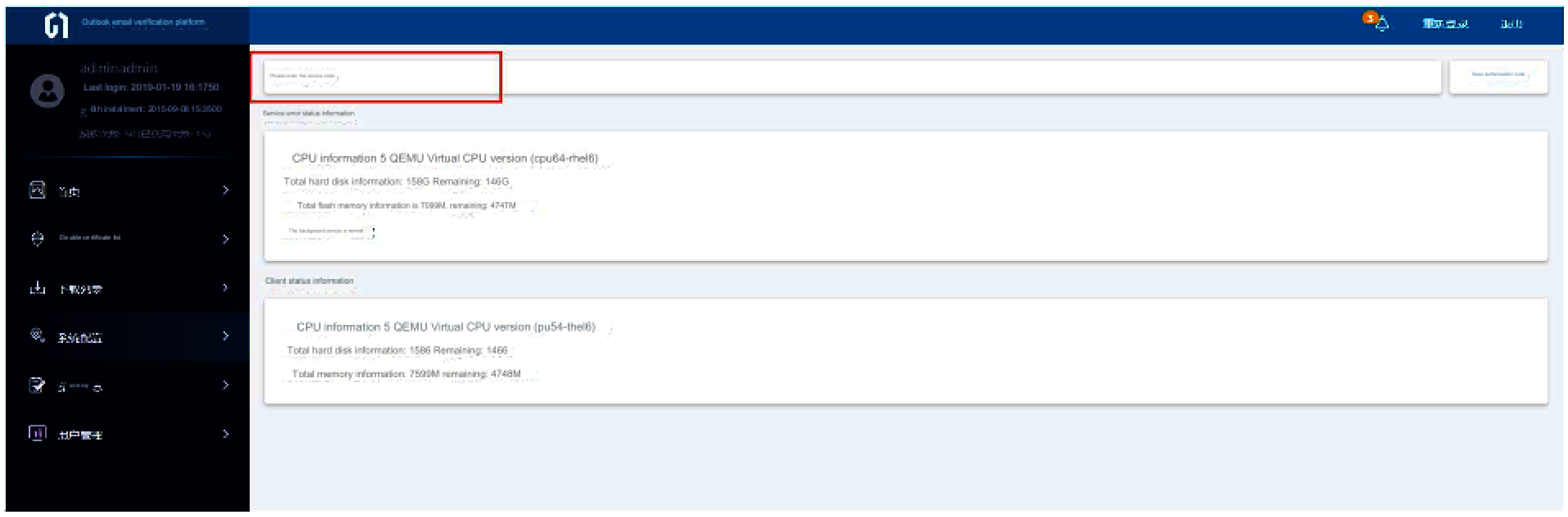
Select the target email account and click the download button in the operation. The emails obtained by this account will be downloaded in a compressed package format. When decompressing, you need to enter the corresponding password to decompress, as shown in the figure below:



[illegible]	Mail	Start and end time	Receive email time	password	schedule	operate
1	[redacted]@hotmail.com	[2018-11-01] --> [2018-11-02]	2018-11-02 15:37:56	ZVBh1HuT	100%	[illegible]

4.4 System configuration

You can see the status of the server and client in the "System Configuration" of the Microsoft mailbox encryption platform. When the account authorization expires or the authorization times are used up, enter a new authorization code to extend the use of the platform, as shown in the figure below:


Outlook email verification platform
重新登录
退出
adminadmin
Last login: 2019-01-19 16:1750
下载列表
系统配置
用户管理

Service error status information

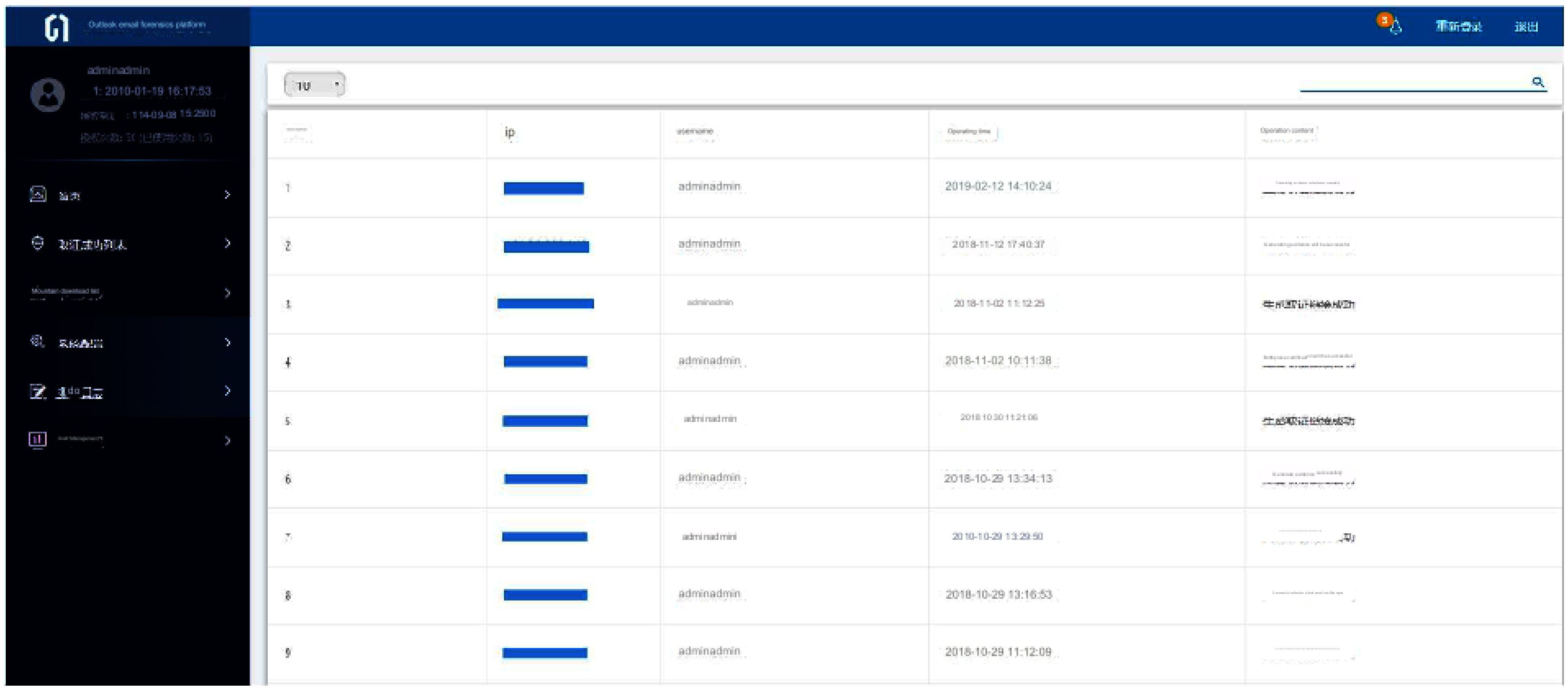
CPU information 5 QEMU Virtual CPU version (cpu64-rhel6)
Total hard disk information: 158G Remaining: 146G
Total flash memory information is 7099M, remaining: 4747M

Client status information

CPU information 5 QEMU Virtual CPU version (pu54-thel6)
Total hard disk information: 1586 Remaining: 1466
Total memory information: 7599M remaining: 4748M

4.5 Operation log

The IP, user name, operation time, and operation content of the account that can be logged in in the "operation log" of the Microsoft mailbox encryption platform, As shown below:

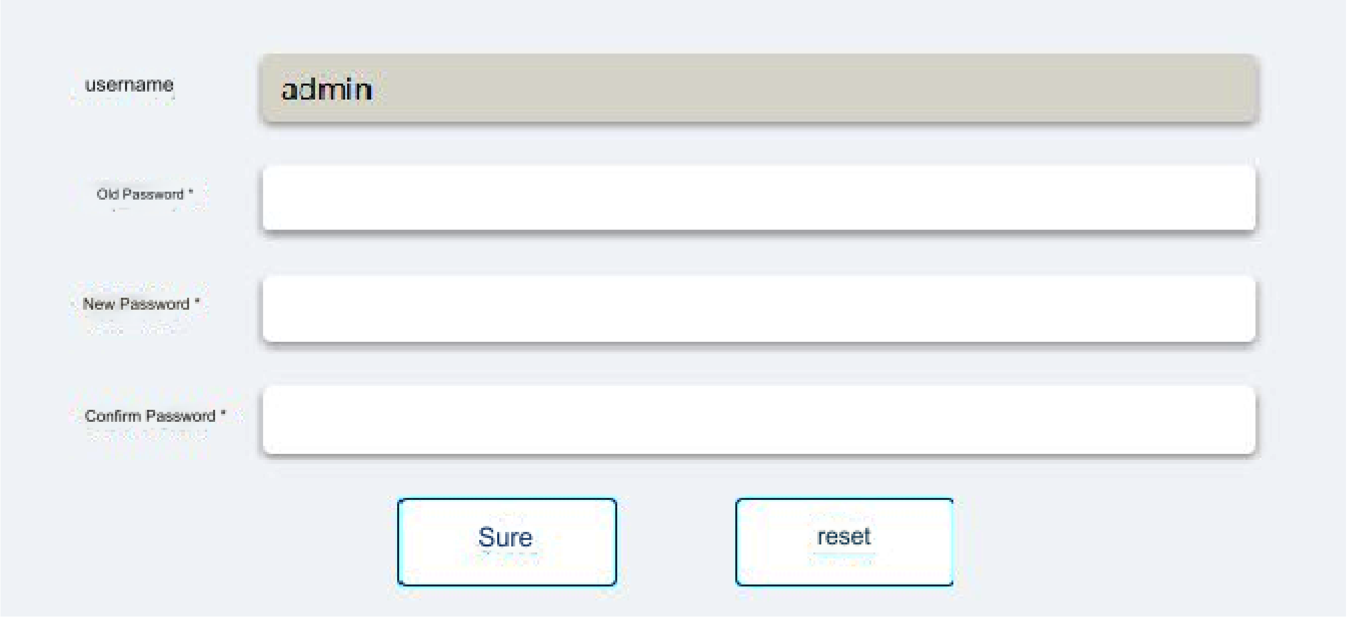


[illegible]	ip	username	Operating time	Operation content
1	[redacted]	adminadmin	2019-02-12 14:10:24	[illegible]
2	[redacted]	adminadmin	2018-11-12 17:40:37	[illegible]
3	[redacted]	adminadmin	2018-11-02 11:12:25	生成取证链接成功
4	[redacted]	adminadmin	2018-11-02 10:11:38	[illegible]
5	[redacted]	adminadmin	2018-10-30 11:21:06	生成取证链接成功
6	[redacted]	adminadmin	2018-10-29 13:34:13	[illegible]
7	[redacted]	adminadmin	2018-10-29 13:29:50	[illegible]
8	[redacted]	adminadmin	2018-10-29 13:16:53	[illegible]
9	[redacted]	adminadmin	2018-10-29 11:12:09	[illegible]

4.6 User management

You can modify the system login name and password for the second login in the "User Management" interface of the Microsoft mailbox encryption platform, as shown in the figure below

Show:


username admin

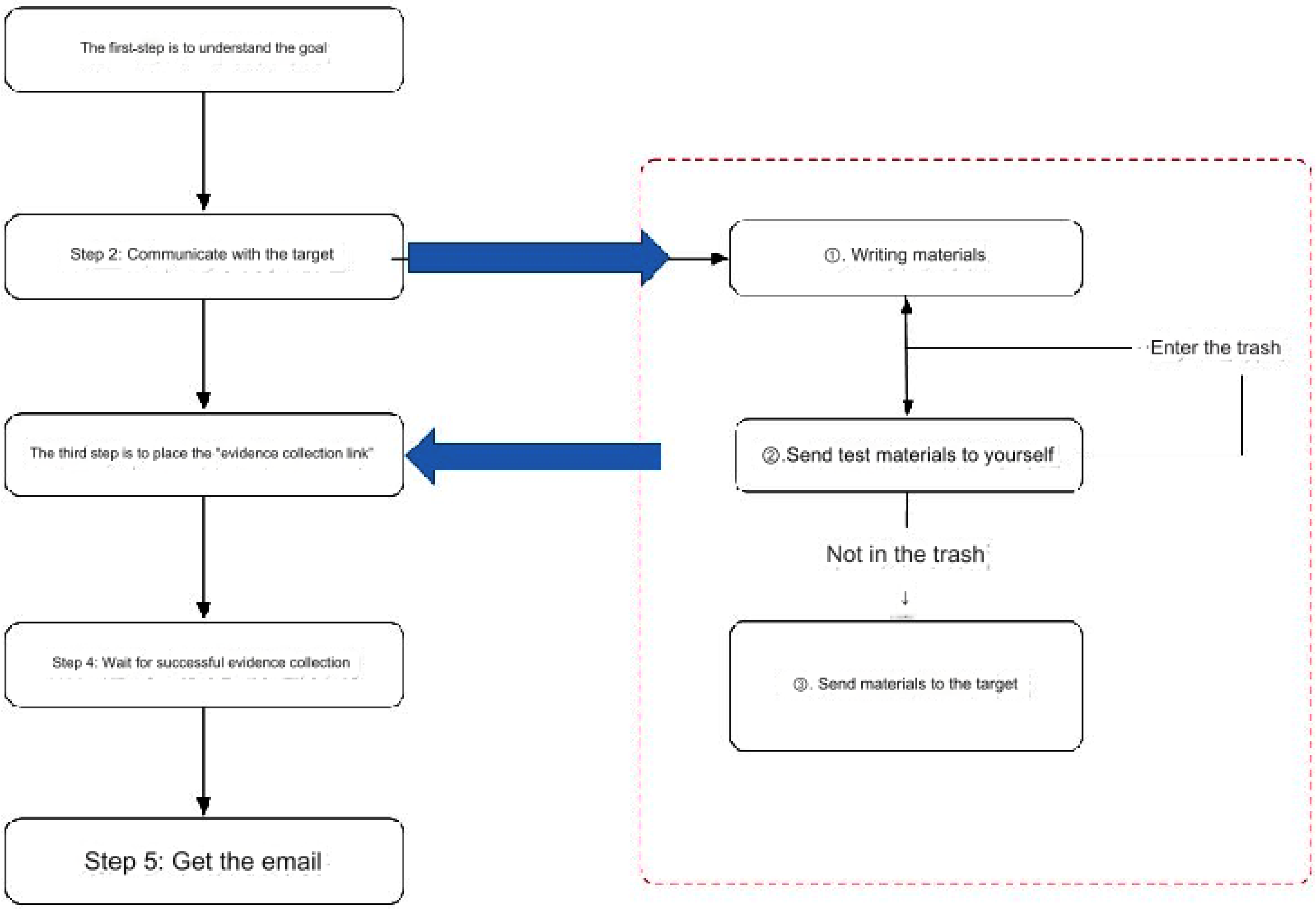
Old Password *

New Password *

Confirm Password *

5 Evidence collection process

In order to ensure the success rate of forensics on the target Outlook email, it is recommended to refer to the following steps to deliver the forensics link:


The first-step is to understand the goal
Step 2: Communicate with the target
The third step is to place the "evidence collection link"
Step 4: Wait for successful evidence collection
Step 5: Get the email
①. Writing materials
Enter the trash
②.Send test materials to yourself
Not in the trash
③. Send materials to the target

Platform operation flow chart

Step 1: It is the first time to use the Microsoft email encryption platform to collect evidence. It is recommended to start with small targets and collect target information;

Step 2: Communicate with the target and build trust;

Step 3: Based on the communication with the target, write the corresponding phishing email and insert the forensic link in the email. To ensure the consistency of the forensic link and the original link, the displayed link in the email can be modified;

Step 4: Send the prepared email to yourself and see if you can successfully receive the email and avoid it being detected as spam by your mailbox;

Step 5: Wait for the evidence collection to be successful and log in to the Microsoft mailbox secret extraction platform to collect the email data.

6 product parameters

category	parameter
Architecture	B/S architecture
Forensic link generation	support
Email encryption	support
Evidence collection time-	Passwords that are not changed are valid for a long time

7 Product Deployment

In order to ensure the stable operation of the entire platform, the server requirements for deploying the Outlook mailbox forensics platform are as follows:

product name	Hardware configuration requirements
Microsoft email secret extraction.platform	1. CPU: dual core 2. Memory: 4G 3. Hard drive: 100G 4. System: Ubuntu1604 5. Bandwidth: ≥4Mbps 6. IP: Deployed overseas, such as Japan, the United States, etc.

8 product advantages

> Ease of use

The system has a B/S architecture. After authorization, users can log in to the system using their login name and password. According to the interface display, a forensic link is generated and sent to the target. After the target clicks on the forensic link, the system automatically collects the evidence from the target. Outlook mailbox data, the whole process is simple to operate and the interface is simple.

> High accuracy

Through the forensic link, the backend system can quickly obtain the session information of his account without the target person having to enter the account password again.

> Exclusive technology

The platform is comprehensively developed and designed based on years of research on the Outlook security mechanism. It can directly bypass Google secondary verification such as login IP and mobile phone verification code, and obtain target email data without active awareness of the target throughout the process.

Microsoft email encryption platform

Product Manual

(V1.0 version in 2022)

Table of contents

1 Introduction

Email is a communication method that provides information exchange through electronic means. It has developed into the most widely used service on the Internet today. E-mail has many characteristics such as fast, environmentally friendly, safe, convenient and multimedia. It can receive emails and store electronic files in various formats. It has become one of the important media tools in the daily life and work communication of netizens.

Hotmail is one of the free email providers on the Internet. Anyone in the world can read it, send and receive emails through a web browser. Outlook mailbox is a free, network-based email portal service owned by Microsoft. Users When you log in to Hotmail, you will also be redirected to your Outlook mailbox, which is a frequently used corporate email service brand. A large number of illegal organizations and criminals use Outlook mailboxes to communicate, organize and spread false statements and create terrorist attacks and other illegal and criminal activities that endanger national security.

2 Requirements analysis

(1) Precisely crack down on illegal crimes

As we all know, Outlook is a highly secure free Internet mail·service launched by Microsoft. Criminals take advantage of this feature of Outlook mailbox to avoid detection by investigators. The Outlook mailbox forensics platform is what Anxun Information has been targeting Outlook for many years. A system developed by Mailbox Security Mechanism is specifically·designed for Outlook mailbox forensics. It can directly bypass the secondary verification without a password and achieve the target person's email data without any sense.

(2) Fill the technical gaps

With the development of information security technology, information warfare has entered a white-hot state. Information has increasingly become the lifeblood of a country and one of the resources that countries are scrambling to seize. In information warfare, stealing enemy information and destroying enemy information systems have become the key to defeating the enemy. At-this stage, a set of evidence collection platforms for Outlook mailboxes are being built to fill this technical gap and help combat illegal crimes. force.