ultraviolet

CONFIDENTIAL

THREAT REPORT:

Career Criminals: The ResumeLooter's Digital Heist Unveiled

Services Performed By:
UltraViolet Cyber
Jacob Wyatt
(443) 351-7630
info@uvcyber.com

Published Date:
02/16/2024

Doc ID: ECORP_SUM_07032023_v1.1

Contents

1 Executive Summary

The ResumeLooters represent a cybercriminal group known for their targeted attacks on job search and recruitment websites. Their motive involves exploiting vulnerabilities in these platforms to steal personal and professional information. This group has gained a reputation for its focus on data that can be used for identity theft, phishing, and further cyber-attacks. ResumeLooters utilize a combination of SQL Injection and Cross-Site Scripting (XSS) attacks to compromise websites. These methods allow them to bypass security measures and access databases containing sensitive user information. They have been known to employ various penetration testing tools, such as SQLmap, Acunetix, Beef Framework, X-Ray, and Metasploit, indicating a high level of technical proficiency and resourcefulness. Their attacks are primarily focused on the Asia-Pacific region, with about 70% of their activities reported in countries like India, Taiwan, Thailand, and Vietnam. However, their operations have a global footprint, affecting websites and users worldwide.

2 Technical Analysis

Here is an overview of some known statistics involving the ResumeLooter’s activities so far:

- The ResumeLooters compromised at least 65 websites between November and December 2023, employing SQL Injection and Cross-Site Scripting (XSS) attacks as their primary tactics.
- They successfully exfiltrated data that included over 2 million unique emails, along with names, phone numbers, employment histories, and other sensitive personal information. This stolen data was subsequently offered for sale on platforms such as Telegram.
- The stolen files contained 2,188,444 rows, of which 510,259 were directly related to user data from job search websites.
- Over 70% of the known victims were in the Asia-Pacific region, including in countries like India, Taiwan, Thailand, and Vietnam. However, the group's activities were not geographically confined, as compromised websites were also identified in Brazil, the USA, Turkey, and Russia.

Below is a diagram (Figure 1) that maps out ResumeLooter’s infrastructure. This illustration was sourced from Group-IB.

© 2023 ULTRAVIOLET. ALL RIGHTS RESERVED.

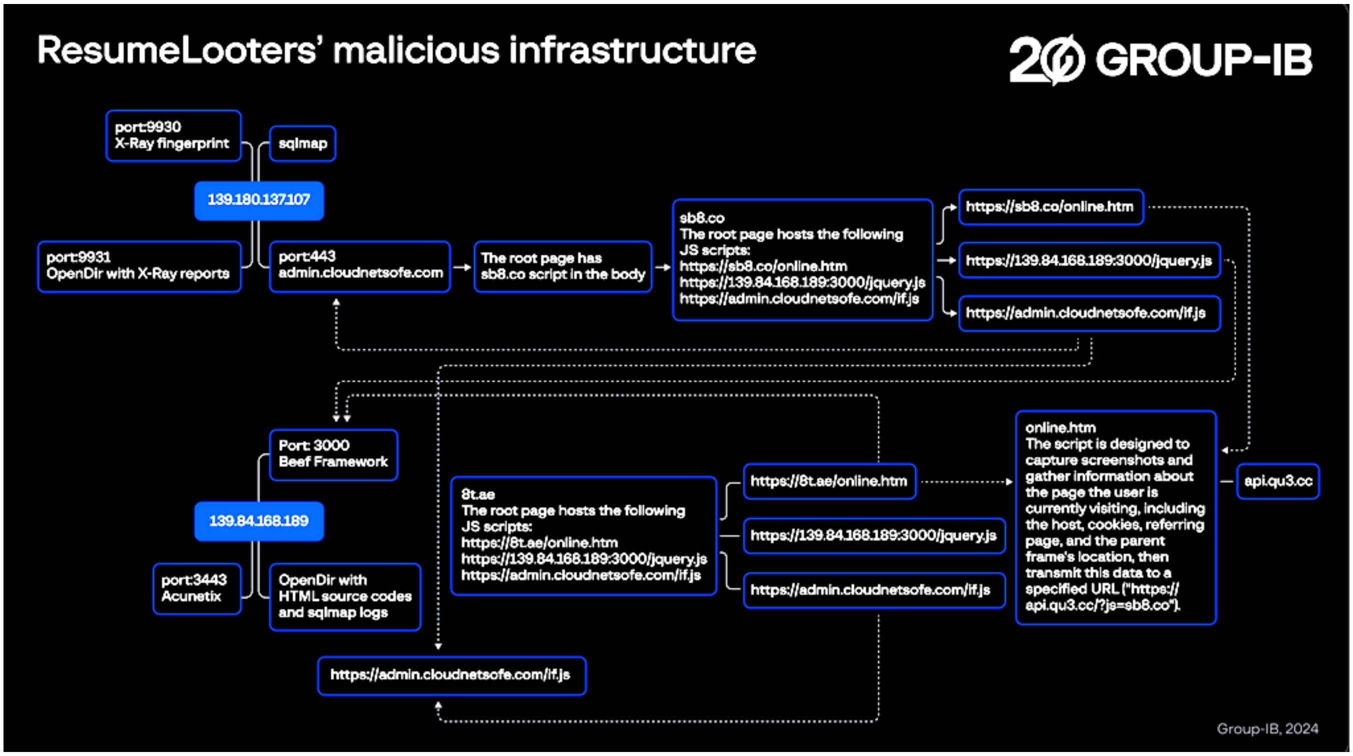
ResumeLooters' malicious infrastructure
GROUP-IB
port:9930
X-Ray fingerprint
sqlmap
139.180.137.107
port:9931
OpenDir with X-Ray reports
port:443
admin.cloudnetsofe.com
The root page has sb8.co script in the body
sb8.co
The root page hosts the following JS scripts:
https://sb8.co/online.htm
https://139.84.168.189:3000/jquery.js
https://admin.cloudnetsofe.com/if.js
https://sb8.co/online.htm
https://139.84.168.189:3000/jquery.js
https://admin.cloudnetsofe.com/if.js
Port: 3000
Beef Framework
139.84.168.189
port:3443
Acunetix
OpenDir with HTML source codes and sqlmap logs
8t.ae
The root page hosts the following JS scripts:
https://8t.ae/online.htm
https://139.84.168.189:3000/jquery.js
https://admin.cloudnetsofe.com/if.js
https://8t.ae/online.htm
https://139.84.168.189:3000/jquery.js
https://admin.cloudnetsofe.com/if.js
online.htm
The script is designed to capture screenshots and gather information about the page the user is currently visiting, including the host, cookies, referring page, and the parent frame's location, then transmit this data to a specified URL ("https://api.qu3.cc/?js=sb8.co").
api.qu3.cc
https://admin.cloudnetsofe.com/if.js
Group-IB, 2024

Figure 1 – ResumeLooters Malicious Infrastructure, (source: https://www.group-ib.com/blog/resumelooters/)

3 What UltraViolet Cyber is Doing

- We are scanning for signs of SQL Injection and Cross-Site Scripting (XSS) attacks in networks. We are also monitoring for unexpected or anomalous network traffic patterns that could indicate command and control (C2) communication or data exfiltration attempts.
- We are monitoring for anomalous activities that suggest unauthorized access or modifications to databases, particularly those storing user profiles and employment information.
- We are continuously analyzing traffic patterns for evidence of data being siphoned to suspicious IP addresses or domains known to be associated with ResumeLooters.

4 What Customers Can Do

- Engage in ongoing cybersecurity awareness programs to educate employees on the specific tactics used by ResumeLooters, including but not limited to, SQL Injection and Cross-Site Scripting (XSS) vulnerabilities.
- Implement network segmentation strategies to restrict unauthorized access and reduce the potential impact of a breach by confining threats to isolated network segments, thus hindering lateral movements by attackers.
- Ensure the timely application of security updates and patches across all systems, software, and web platforms to mitigate vulnerabilities.

© 2023 ULTRAVIOLET. ALL RIGHTS RESERVED.

5 References

- "ResumeLooters: Cyber Threats and Solutions." *Group-IB*, 1 Feb. 2024, www.group-ib.com/blog/resumelooters/.
- "ResumeLooters Attackers Steal Millions of Career Records." *Dark Reading*, Elizabeth Montalbano 02/06/2024, www.darkreading.com/remote-workforce/-resumelooters-attackers-steal-millions-career-records.
- "ResumeLooters Steal Millions of Unique Emails from Multiple Sites." *Cyware*, 02/09/24, www.cyware.com/news/resumelooters-steal-millions-of-unique-emails-from-multiple-sites-b8f0f81b.

© 2023 ULTRAVIOLET. ALL RIGHTS RESERVED.