Infinity
External Risk Management

AKIRA PUBLISHED OVER 30 NEW VICTIMS ON THEIR DLS

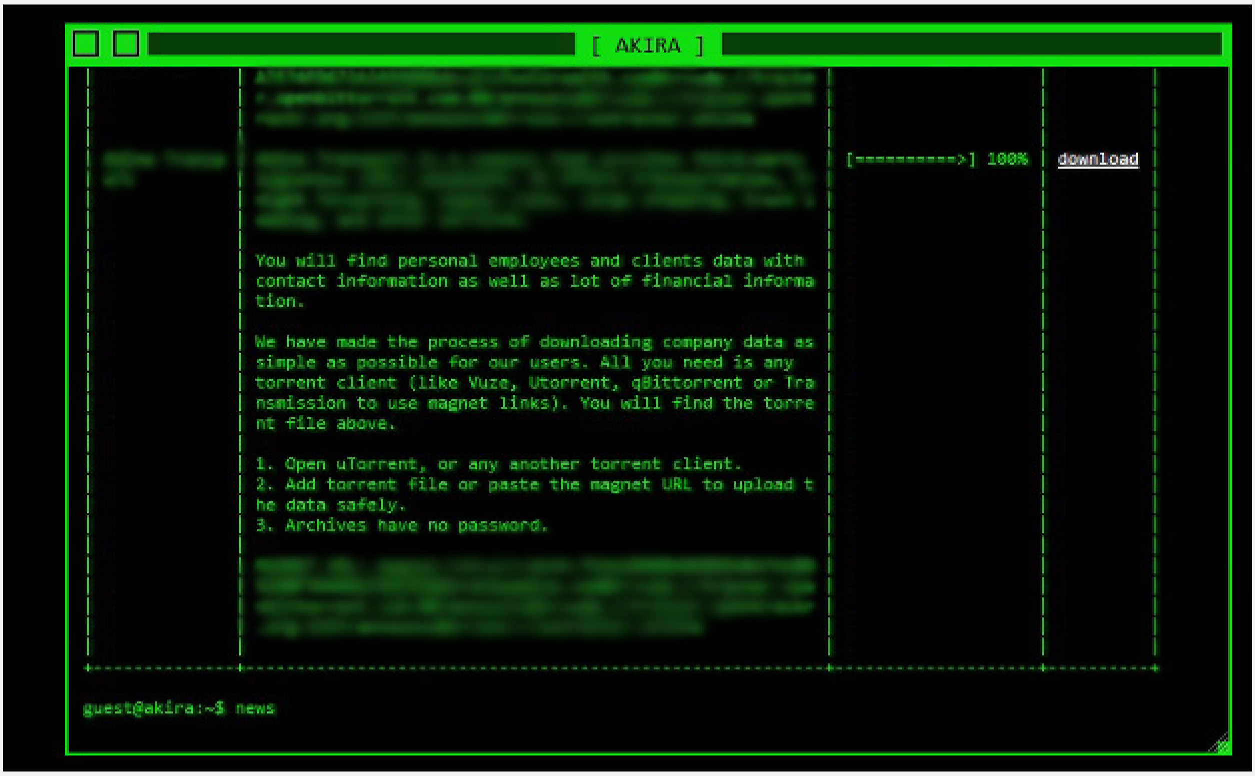
INTRODUCTION

The Akira ransomware group has been active since March 2023, targeting diverse industries across North America, the UK, and Australia. Operating as a Ransomware-as-a-Service (RaaS) model, Akira employs a double-extortion strategy by stealing sensitive data before encrypting it. According to their leak site, the group claims to have compromised over 350 organizations.

From November 13 to 14, the Akira ransomware group posted over 30 new victims on their data leak site, marking their highest single-day total since they began operations in March 2023. This milestone represents a record-breaking escalation in their activities and the volume of leaks shared in one day.

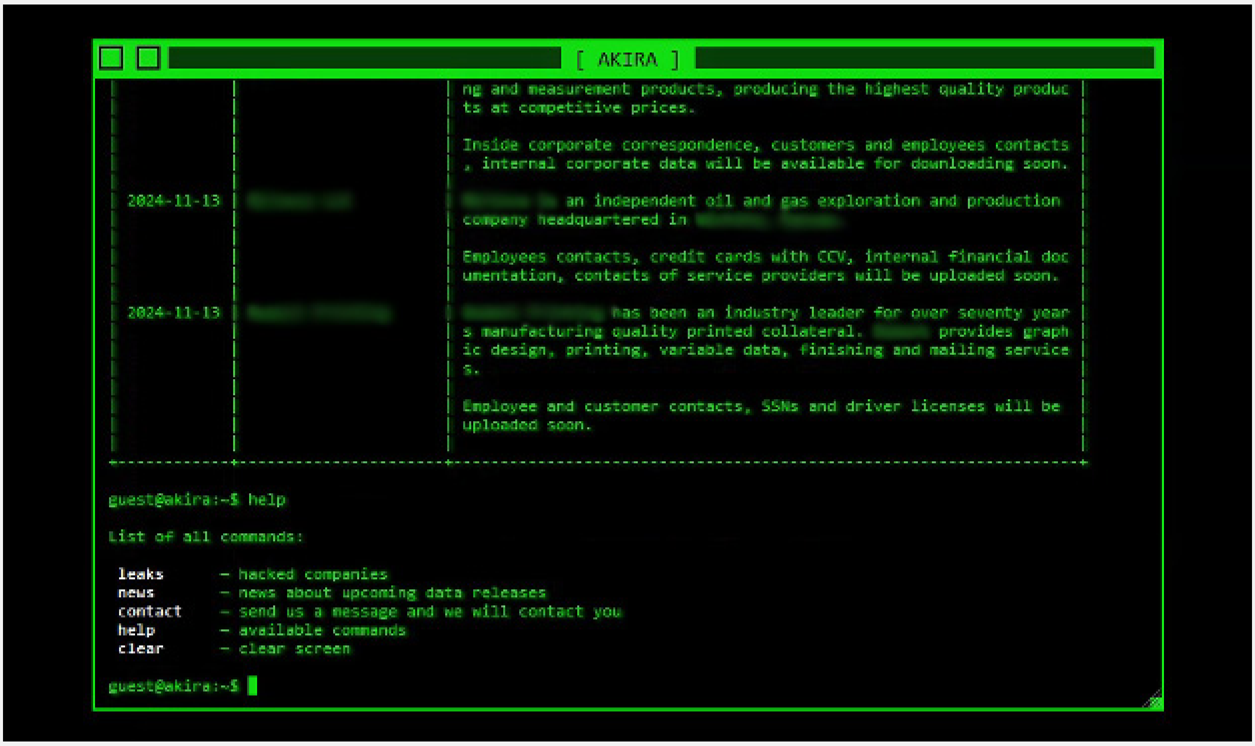
The Akira ransomware blog is organized into five sections. The **"Leaks"** section lists victims who refused to pay the ransom, leading the group to publicly release their encrypted data. The **"News"** section highlights new victims, likely organizations currently engaged in ransom negotiations.

In the 'Leaks' section we've seen 3 victims that already been published on the 'News' section, and 29 new ones. In the 'News' section, we've seen 3 new victims. Which basically means that 32 new victims were published in the group's DLS, and three more refused to pay the ransom and were added to the 'Leaks' section.



```
[redacted]

[redacted]    [redacted]                                  [==========>] 100%

              You will find personal employees and clients data with
              contact information as well as lot of financial informa
              tion.

              We have made the process of downloading company data as
              simple as possible for our users. All you need is any
              torrent client (like Vuze, Utorrent, qBittorrent or Tra
              nsmission to use magnet links). You will find the torre
              nt file above.

              1. Open uTorrent, or any another torrent client.
              2. Add torrent file or paste the magnet URL to upload t
              he data safely.
              3. Archives have no password.

              [redacted]

guest@akira:~$ news
```

Figure 1: Leaks section



```
|            |                            | ng and measurement products, producing the highest quality produc |
|            |                            | ts at competitive prices.                                          |
|            |                            |                                                                    |
|            |                            | Inside corporate correspondence, customers and employees contacts |
|            |                            | , internal corporate data will be available for downloading soon. |
|            |                            |                                                                    |
| 2024-11-13 | [redacted]                 | [redacted] an independent oil and gas exploration and production   |
|            |                            | company headquartered in [redacted]                               |
|            |                            |                                                                    |
|            |                            | Employees contacts, credit cards with CCV, internal financial doc |
|            |                            | umentation, contacts of service providers will be uploaded soon.  |
|            |                            |                                                                    |
| 2024-11-13 | [redacted]                 | [redacted] has been an industry leader for over seventy year      |
|            |                            | s manufacturing quality printed collateral. [redacted] provides graph |
|            |                            | ic design, printing, variable data, finishing and mailing service |
|            |                            | s.                                                                 |
|            |                            |                                                                    |
|            |                            | Employee and customer contacts, SSNs and driver licenses will be  |
|            |                            | uploaded soon.                                                     |
|            |                            |                                                                    |
+------------+----------------------------+--------------------------------------------------------------------+

guest@akira:~$ help

List of all commands:

 leaks      - hacked companies
 news       - news about upcoming data releases
 contact    - send us a message and we will contact you
 help       - available commands
 clear      - clear screen

guest@akira:~$
```

Figure 2: News Section

WHO ARE THE VICTIMS?

Of the 35 total posts, 25 originate from the United States. Canada accounts for two, while the remaining posts come from Uruguay, Denmark, Germany, the United Kingdom, Sweden, the Czech Republic, and Nigeria.

The Business Services sector is the most frequently targeted, with 10 organizations affected. Other impacted industries include Manufacturing, Construction, Retail, Technology, Education, and Critical Infrastructure.

These findings align with trends observed over the past two years, where the United States remains Akira's primary target, and Business Services continues to lead as the most targeted sector globally.

SIMILAR INCIDENTS FROM THE PAST

Akira is not the only ransomware group to post such a large number of victims in a single day. For instance, on May 6, 2024, LockBit released details of 57 new victims on their recently launched data leak site within just one hour, followed by two more victims on May 7. This highlights a growing trend among ransomware groups to escalate their operations and exert pressure through mass disclosures.

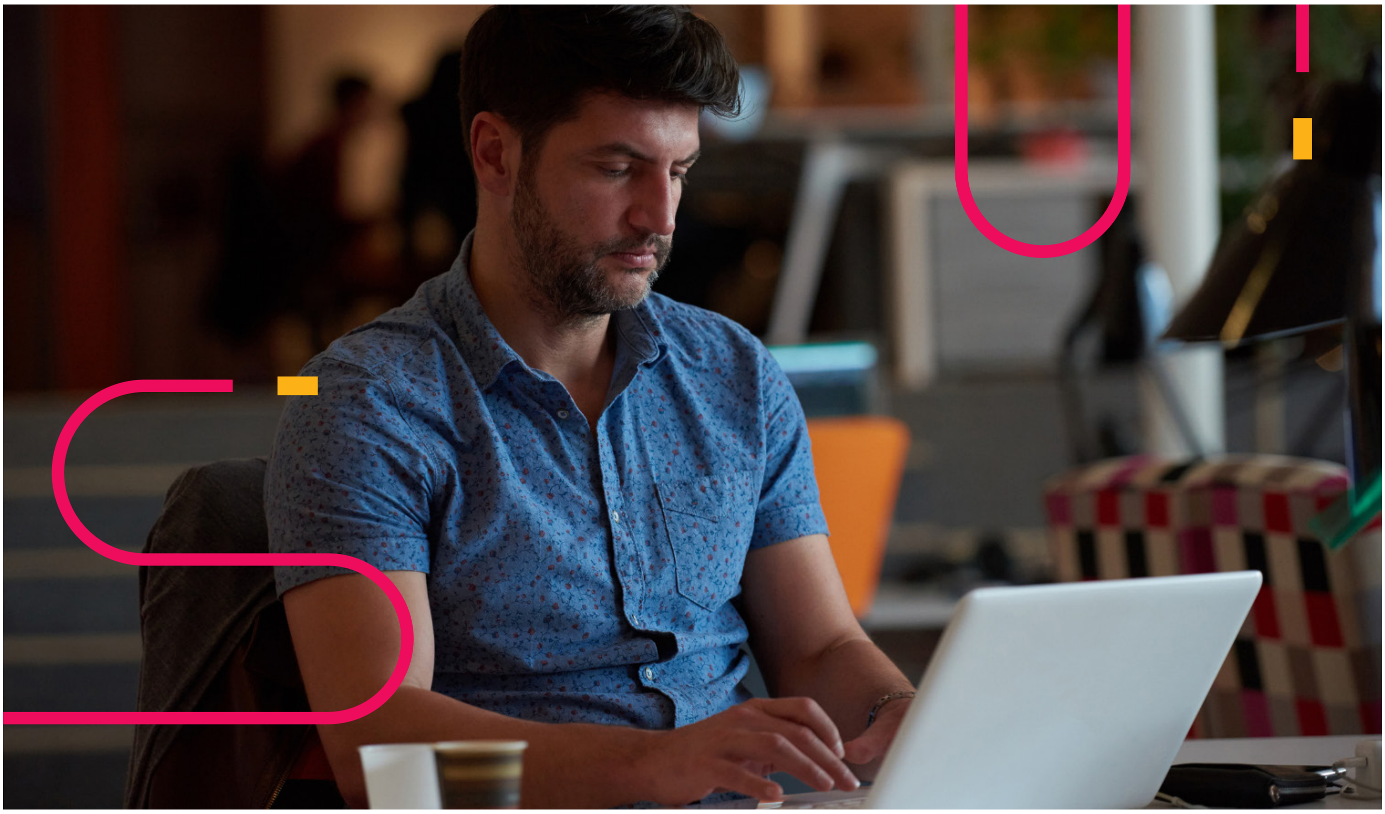
From that moment the activity of the Lockbit group decreased, where the main hit was in February at Operation Cronos, where Law enforcement dismantled LockBit's infrastructure, including 34 servers hosting the data leak site and its copies, along with stolen victim data, cryptocurrency addresses, 1,000 decryption keys, and the affiliate panel.

Is this means that Akira is shooting their last bullet in the barrel?
Probably not.

CONCLUSION

In April, Akira made headlines after the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI reported the group had earned $42 million from 250 attacks since March 2023, averaging $3.5 million in monthly revenue.

Akira remains a dominant player in the ransomware landscape, targeting hundreds of victims worldwide. Its activity is expected to grow further, especially after achieving a record-breaking month in the number of victims and surpassing the total attacks for 2023 in just a few months. This highlights their aggressive and expanding operations in the cybercrime ecosystem.



ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Check Point External Risk Management to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

For more information visit: https://cyberint.com / checkpoint.com/erm