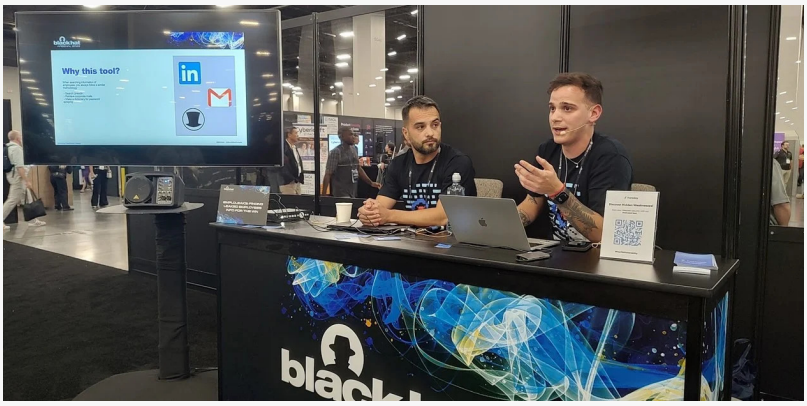
EmploLeaks: The Open-Source Tool to Detect Leaked Employees Information and Enhance Your Company's Security

EmploLeaks scours various platforms to compile a list of employees and cross-references their emails, checking for potential password exposure.



Our team in BlackHat Arsenal

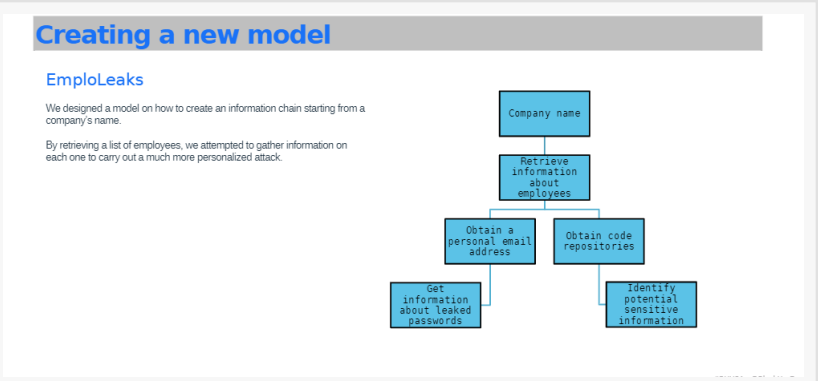
MIAMI, FLORIDA, UNITED STATES, July 11, 2024 /EINPresswire.com/ -- Emploleaks is an open source tool developed by Faraday Security researchers. EmploLeaks extracts valuable insights by scouring various platforms, to compile a comprehensive list of employees associated with a given company and cross-reference these email with databases like COMB and other internet sources, checking for potential password exposure.

> “We believe that by making this tool openly available, we can help organizations proactively identify and mitigate the risks associated with leaked employee credentials”.”
>
> *Gabriel Franco*

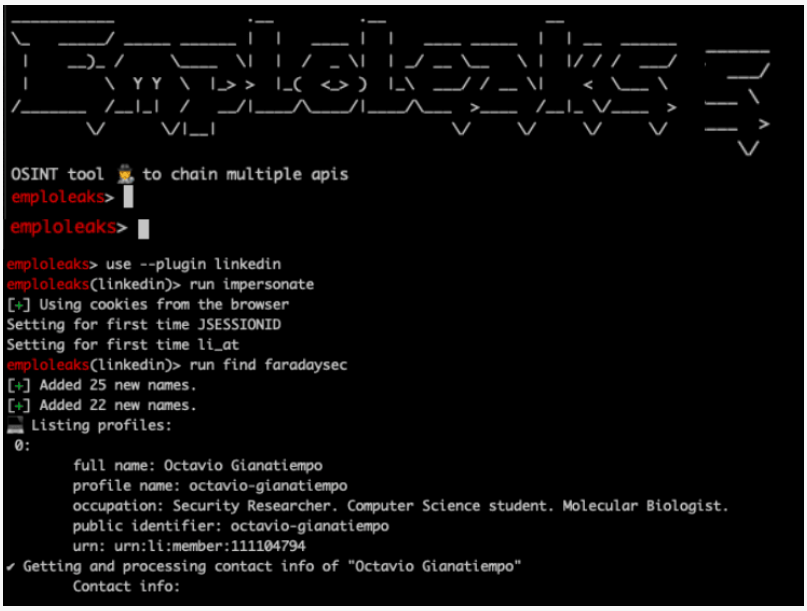
Faraday started as an open-source project to become a cybersecurity company that offers a vulnerability management platform and red team services helping organizations and security teams orchestrate and automate their security process. Their strong research team has consistently presented new discoveries at DefCon and Black Hat conferences for almost five years. This past year, they presented an open source tool at Black Hat Arsenal to detect leaked passwords in companies employees.

During red team assessments, Faraday’s Red Team and Research teams found that personal information leaked in breaches can pose a significant risk to their clients. It is often the case that personal passwords are reused in enterprise environments. But even when they aren’t reused, these passwords, in conjunction with other personal information, can be used to derive working credentials for employer resources.

Collecting this information manually is a tedious process. Therefore, their ex Research leader Javier Aguinaga, and Head of Security Services Gabriel Franco developed a tool that helps them quickly identify any leaked employee information associated with their personal email address. The tool proved to be incredibly useful for the Faraday team when used internally. Moreover, they quickly recognized the potential benefits it could also offer to other organizations facing similar security challenges. As a result, they made the decision to open-source the tool.



Creating a new model



Our open-source tool

EmploLeaks enables the collection of personal information through Open-Source Intelligence techniques. It starts by taking a company domain and retrieving a list of employees from LinkedIn. Subsequently, it gathers data on individuals across various social media platforms (currently developing Twitter modules and other social networks) such as LinkedIn and GitHub more, to obtain company email addresses. Once these email addresses are found, the tool searches through a COMB database (stands for compilation of many breaches, a large list of breached data) and other internet sources to check if the user's password has been exposed in any breaches.

Also, Emploleaks is now integrated with Faraday Advance Scan, which will let you know if anyone in your company has a breached password.

"Initially, we developed an internal tool that displayed great potential, leading us to make it open source. Since then, we have continually developed the tool, with the latest version recently pushed to the repository. Our current focus is on ensuring that the application flow is efficient, and we are diligently addressing any bugs that arise as soon as possible. This is an ongoing process, and we are committed to providing a high-quality tool that is reliable and meets the needs of the community. As we proceed with development, we welcome feedback and contributions from users to help us enhance the tool further." completes Franco.

Try Emploleaks.

Get to know all of Faraday Security projects and tools.

Faraday Security
Faraday Security
+1 904-715-4284
email us here
Visit us on social media:
X
LinkedIn
Instagram
YouTube
TikTok
