UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 6-K

**REPORT OF FOREIGN PRIVATE ISSUER PURSUANT TO RULE 13a-16
OR 15d-16 OF THE SECURITIES EXCHANGE ACT OF 1934**

For the month of April, 2018

Commission File Number 000-26495

Cyren Ltd.

(Translation of Registrant's name into English)

1 Sapir Road, 5th Floor, Beit Ampa, P.O. Box 4014, Herzliya 46140, Israel
(Address of Principal Executive Offices)

Indicate by check mark whether the registrant files or will file annual reports under cover of Form 20-F or Form 40-F.

Form 20-F ☒   Form 40-F ☐

Indicate by check mark if the registrant is submitting the Form 6-K in paper as permitted by Regulation S-T Rule 101(b)(1):___

Indicate by check mark if the registrant is submitting the Form 6-K in paper as permitted by Regulation S-T Rule 101(b)(7):___

On April 9, 2018, the Registrant issued a press release announcing the release of new powerful capabilities for enterprises to combat new cryptomining risks and impostor email threats. A copy of the press release is annexed hereto as Exhibit 1 and incorporated herein by reference.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

Cyren Ltd.
(Registrant)

Date: April 9, 2018

By: /s/ J. Michael Myshrall
J. Michael Myshrall
Chief Financial Officer

Exhibit 1

Cyren's Latest Launch Takes Aim at New Cryptomining Risks and Impostor Email Threats

McLean, VA – April 9, 2018 – Moving to help businesses stay ahead of new threats related to cryptocurrency mining and impostor email attacks, Cyren (NASDAQ: CYRN) announced today the availability of new powerful capabilities for enterprises to combat these rapidly growing security risks. The capabilities are offered as part of a new release of the Cyren Cloud Security platform, which integrates web security, email security, DNS security and cloud sandboxing on a single, globally operated security cloud.

"Follow the money, and you will find cybercrime – sophisticated, well-funded criminals are opportunists, and are constantly looking for new pathways into businesses," said Ben Carmi, senior vice president of product at Cyren. "Our responsibility is to innovate ahead of the curve in order to protect our customers and their employees. Our unified cloud platform allows us to swiftly deploy capabilities to address new threats head-on. That's something that traditional security appliances simply can't do. Combining constant innovation with the insight we gain from inspecting 25 billion security transactions and blocking more than 300 million threats each and every day, we are able to rapidly thwart new threats as they emerge and evolve."

Cryptocurrency Mining: The Next Threat Frontier?
Fueled by soaring cryptocurrency prices during 2017, in-browser cryptocurrency mining is being discussed as an alternative business model for advertising-driven web sites. Cyren researchers reported a 725 percent surge in cryptocurrency mining found during a global tracking study conducted from October 2017 through January 2018. While some sites do ask for a visitor's explicit permission, most web pages running JavaScript programs to mine cryptocurrency do so without the user's permission, a tactic referred to as "cryptojacking," and in many cases this is being done by scripts injected by cybercriminals. Such scripts running in a single browser page typically use 60-70% of a visitor's CPU, with reports as high as 100%. Forms of mining malware and bots have also appeared and are being targeted at business computing resources by many of the same criminal gangs associated with ransomware and other threats, using the same distribution methods.

Cyren has developed specific functionality for enterprises looking to understand the scope of any cryptomining and unwanted cryptojacking activity in their employees' web use, and to mitigate any potential impact. Cyren has added a cryptocurrency mining category to the URL classification system in Cyren Web Security that contains websites, URLs and cloud applications known to run mining scripts, allowing companies to report on and block access to this category by user, group or across the organization.

Impostor Protection – Advanced Email Security
The latest release also contains enhancements addressing business email compromise (BEC) attacks, which are on the rise. While many criminal gangs use networks of infected computers (botnets) to send out massive volumes of phishing emails and malware attachments, BEC attacks are well-researched, well-crafted and targeted to a selected list of recipients. "Impostor" emails appear as if they have been sent by the CEO or other executive, frequently addressed to members of a company's finance or HR team. While small in number, these attacks can be high in impact, successfully evading legacy security appliances and deceiving employees. Cyren Email Security quickly identifies and blocks these kinds of attacks automatically.

Cloud Access Security - Shadow IT Visibility & Control
Cloud application adoption by business users continues to grow rapidly, and the proliferation of both sanctioned and unsanctioned (or "Shadow IT") cloud applications is often times problematic. Cloud applications may lack the security and governance needed to protect confidential data, and some may harbor malicious code that extracts sensitive information or credentials. As such, cloud access security is becoming an essential element of any cloud security strategy, and security and risk management leaders are looking for both shadow and sanctioned IT discovery, as well as a consolidated view of cloud service usage throughout the organization.

As part of Cyren Web Security, the company has enhanced cloud application access controls to enable IT organizations to quickly obtain full usage visibility and easily implement policy-based access controls for more than 2,500 of the most frequently used cloud applications. Available as part of the Cyren Web Security service, the cloud access security capability supports shadow IT discovery and control, providing full reporting on application usage by each user, and enabling security teams to block access to specific applications or application classes on a user- or group- basis.

To learn more, see a demo or trial these new capabilities, go to https://www.cyren.com/get-started

About Cyren
More than 1.3 billion users around the world rely on Cyren's 100% cloud internet security solutions to protect them against cyberattacks and data loss every day. Powered by the world's largest security cloud, Cyren (NASDAQ and TASE: CYRN) delivers fast time to protection from cyber threats with award-winning security as a service for web, email, sandboxing, and DNS for enterprises, and embedded threat intelligence solutions for security vendors and service providers. Customers like Google, Microsoft and Check Point are just a few of the businesses that depend on Cyren every day to power their security. Learn more at Cyren.

Blog: blog.cyren.com
Facebook: www.facebook.com/CyrenWeb
LinkedIn: www.linkedin.com/company/cyren
Twitter: www.twitter.com/CyrenInc or twitter.com/cyren_ir

Company Contact:
Mike Myshrall, CFO
Cyren
+1.703.760.3320
mike.myshrall@cyren.com

Media Contact:
Matthew Zintel
Zintel Public Relations
+1.281.444.1590
matthew.zintel@zintelpr.com