Feroot Announces Next-Generation Cyber-defence Platform to Eliminate Web Skimming Risks and Gaps Exploited by Magecart

As data collection grows on the web, CISO's, Digital and Risk executives cite the need for a simple, reliable and scalable way to protect data and brand safety.

Eliminate the easy way in

TORONTO, ONTARIO, CANADA, February 10, 2020 /EINPresswire.com/ -- Feroot, developer of award-winning data protection tools that provide comprehensive visibility and control for customers over their data security on the web, today introduced the Feroot platform with new capabilities. The new release enables organizations to fully identify their attack surface on the web, activate pro-active defenses to safeguard customer and employee data to protect business continuity.

The Feroot platform continuously maps all web-exposed assets in an organization, to identify their business context (i.e., web pages where organizations are ingesting personal information like credit card numbers, social insurance, billing, financial and health data), detect intrusion attempts, and prioritize attack vectors. Additionally, it activates defenses to protect data against Magecart digital skimming attacks, cybersecurity, and compliance risks.

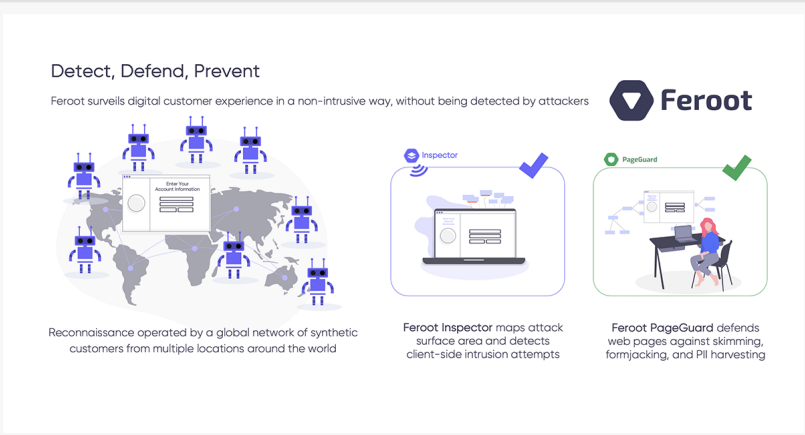
> "Modern web development makes the use of third-party controlled scripts very common. Recent Magecart breaches show that these scripts also leave many organizations vulnerable to e-skimming attacks."
> *Ivan Tsarynny, Feroot CEO and Co-Founder.*

The Feroot platform deploys a unique reconnaissance process supported by a globally operated network of synthetic customers that continuously and intelligently use web applications and websites from multiple locations around the world. Feroot's approach enables surveillance of digital customer experience in a non-intrusive way, without being detected by attackers. This outside-in approach helps reveal the presence of malicious activities, including JavaScript sniffers, i.e., keystroke recorders at the browser-level. Additionally, it discovers the full extent of the client-side attack surface, which presently is outside of today's security-edge and is missed by existing security approaches.

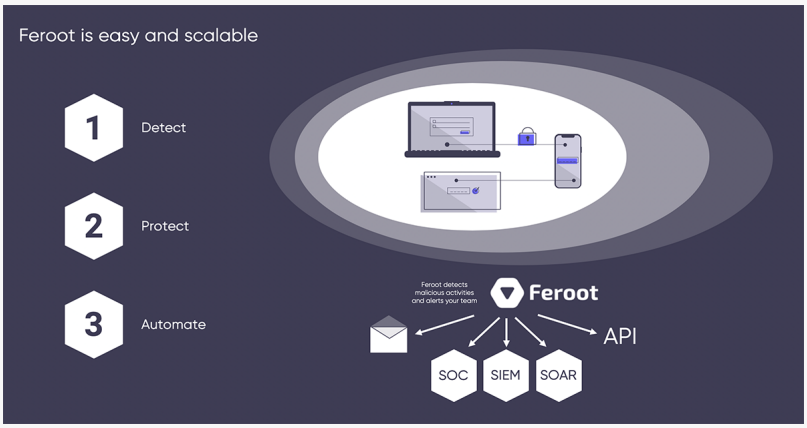
New capabilities enable customers to prevent e-skimming breaches by the latest generation of skimming exploits that use sophisticated multi-stage attacks with side-loaded JavaScript code, anti-forensic, and detection evasion techniques. This release advances the Feroot's unique ability to protect organizations and their customer data against security and compliance risks.

Newly added capabilities include:

• Autonomous discovery and reporting of all third-party business tools that are chain-loaded and side-loaded by each web page and can be used in a supply chain skimming attacks – including chatbots, digital ad pixels, marketing analytics tools, marketing tag managers, sales enablement tools, customer success platform, and all other proprietary and open-source JavaScript code and libraries.
• Data Access Policy engine to enable centralized control the level of access and permissions of all JavaScript code including all third-party code loaded by each web page
• A new application programming interface (API) to streamline security, integrations, and automation using Feroot, making the platform even more developer-friendly.



Detect, Defend, and Prevent e-skimming Magecart attacks



Easy and scalable

"Great digital customer user experience (UX) helps retain existing customers, gain new customers, upsell, cross-sell, and is the force behind most organization's cash flow. Today's organizations rely on third-party scripts and libraries to implement business-driven functionalities and features such as analytics, marketing retargeting, live chat, forms, or shopping carts." - said Ivan Tsarynny, Feroot CEO and Co-Founder. "Modern web development makes the use of third-party controlled scripts very common if unavoidable at all. These scripts also leave many organizations vulnerable to skimming attacks, as seen in the wave of breaches over recent weeks. The growing sophistication of Magecart attack tools and new vectors of attacks are blindsiding legacy security solutions and outpacing capabilities of today's tools, leaving even highly security-conscious organizations vulnerable."

Availability
The newly released Feroot platform is now generally available to all current and new customers.

About Feroot
Feroot is dedicated to keeping the web safe and compliant. The Feroot cyber-defense platform combines behavior-based intrusion detection with proactive defenses that prevent digital skimming and other emerging threats. It provides actionable insights, enables collaborations between security, privacy, marketing, and other departments to help organizations protect business continuity and brand safety.

Ivan Tsarynny
Feroot
+1 408-692-6429
email us here