

# Feroot Platform Honeypot Customer Decoys Ambush Magecart Skimming Attackers

*Forcing attackers to engage with the decoy users and customers provides cyber defenders time to remediate and prevent further risks.*

TORONTO, ONTARIO, CANADA, February 25, 2020 /EINPresswire.com/ -- [Feroot](#), an award-winning company and the leader in detection of the [client-side](#) cybersecurity threats within digital user experience, today announced new capabilities in its threat detection platform. The latest release provides a comprehensive deception fabric operated by a global network of honeypot customers (decoys) that lure and trigger malicious code activities, including [Magecart](#) skimming attacks. This deception approach enables early detection, visibility into the shadow threats, and proactive risk mitigation. Newly released threat detection capabilities will also serve as a powerful early warning of attacks on the digital user experience via unmanaged and uncontrolled third-party code.

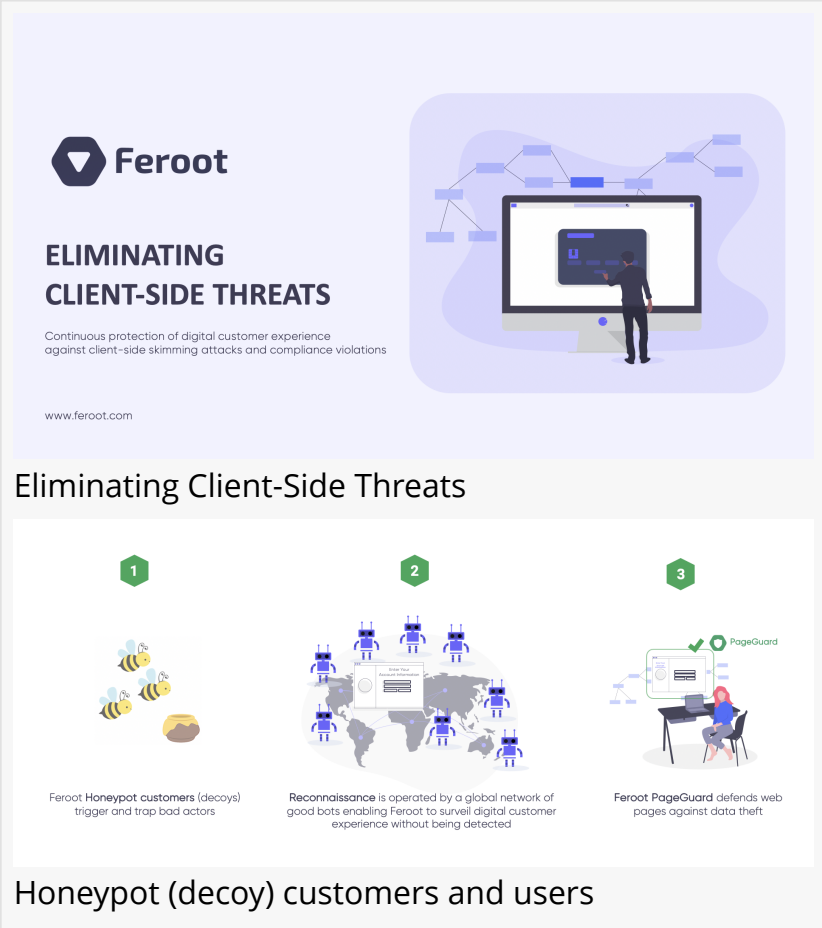
“Protecting digital user experience and preventing client-side data breaches is a critical concern for organizations of all sizes. Drive-by skimming and other types of Magecart attacks are revealing that attackers can breach hundreds of organizations at once by compromising any widgets that are loaded by modern websites and web applications.” - said Vitaliy Lim, Feroot CTO, and Co-Founder.



Little widgets is a big problem. The honeypot user approach allows the detection of Magecart attacks by triggering the skimming of decoy customer's information.”

*Vitaliy Lim, Feroot CTO and Co-Founder.*

before any serious damage is done.



The infographic is titled "ELIMINATING CLIENT-SIDE THREATS" and features the Feroot logo. It includes a sub-headline: "Continuous protection of digital customer experience against client-side skimming attacks and compliance violations" and the website "www.feroot.com". Below the title is a diagram showing a person at a computer screen with a network diagram above it. The main content is a three-step process:

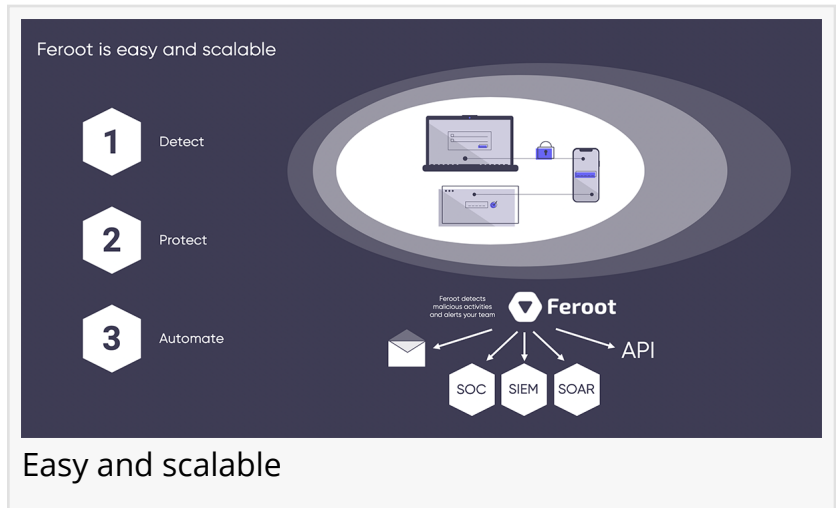
- 1** Feroot Honeypot customers (decoys) trigger and trap bad actors (illustrated with bees).
- 2** Reconnaissance is operated by a global network of good bots enabling Feroot to surveil digital customer experience without being detected (illustrated with a globe and blue bots).
- 3** Feroot PageGuard defends web pages against data theft (illustrated with a person at a computer and a shield).

The bottom of the infographic is labeled "Honeypot (decoy) customers and users".

The honeypot attacker deception concept has been used in law enforcement, military, and counterintelligence domains for a long time. Placing honeypot assets as decoy databases, endpoints, and other types of traditional digital assets is an effective way to misdirect and trap attackers. The introduction of honeypot deception to the cyber defense of the digital user experience is changing the asymmetry of cyber-attack. It turns the entire digital experience into a minefield for bad actors. This approach allows early detection and derailing of client-side attacks

By turning the entire digital UX into a data trap, information security teams can go on the counter offense against attackers. In addition to analyzing the context of the skimming attack, the Ferroot platform also assists with client-side breach forensics, remediation, and prevention.

Ferroot honeypot customer approach is tackling the client-side security challenges head-on by turning malicious code activities such as web skimming attempts against attackers.



The Ferroot Honeypot decoy user solution gives clear visibility into security, data governance, and compliance of digital user experience. These capabilities include detection of:

- Theft of login credentials -- decoy users lure and trap keystroke sniffers.
- Theft of credit card payment information -- decoy customers trigger and trap Magecart payment card skimming attacks.
- Backdoors that skimming attackers can take to comprise digital experience -- organizations gain visibility and insights needed to remove risks created by side-loaded or chain-loaded code.

Ferroot is continually strengthening its client-side threat detection capabilities to learn more about the Ferroot Honeypot-based Client Side Threat Detection Platform visit the Ferroot website at [www.ferroot.com](http://www.ferroot.com).

#### About Ferroot

Ferroot is dedicated to keeping business on the web safe, compliant and innovation-friendly. The Ferroot 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.

All trademarks are the property of their respective owners.

Ivan Tsarynny  
Ferroot Privacy  
+1 408-692-6429

[email us here](#)

Visit us on social media:

[Twitter](#)

[LinkedIn](#)

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2020 IPD Group, Inc. All Right Reserved.