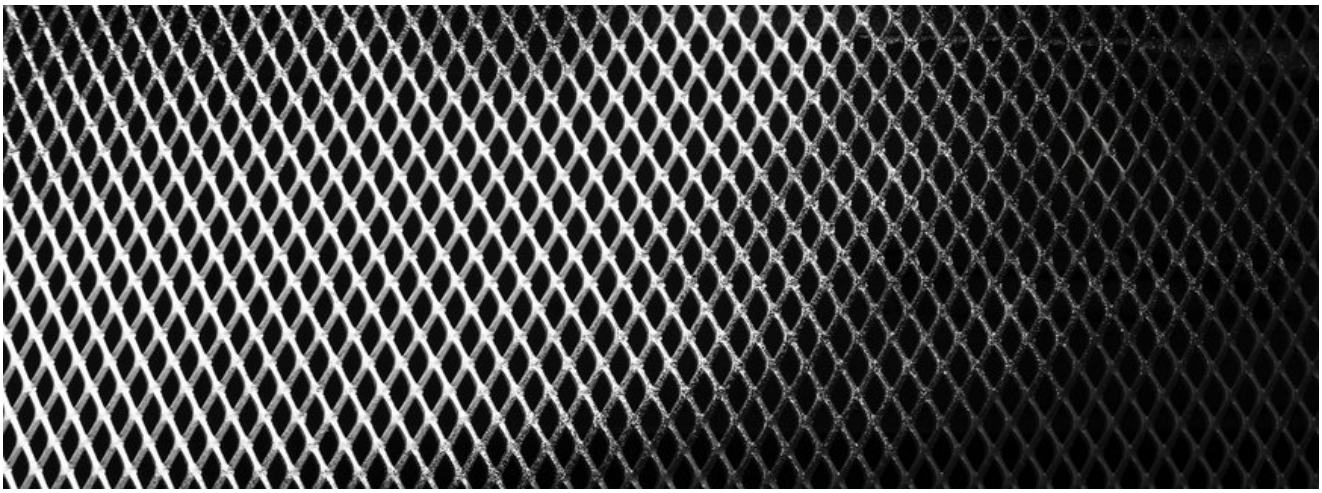
New Analysis Puts Magecart Interconnectivity into Focus

riskiq.com/blog/labs/magecart-medialand/

January 14, 2021



Labs Magecart

January 14, 2021

By Team RiskIQ

RiskIQ's recent analysis of Magecart infrastructure has shown its massive scale and put its interconnectivity into focus. Our most recent research takes two email addresses evoking the name of one of the most prominent bulletproof hosting providers on earth and ties them to newly discovered batches of Magecart infrastructure. From there, we show how this infrastructure overlaps with previously reported Magecart activity and highlight some common Magecart operator practices that can help researchers identify skimming infrastructure.

Media Land is King

Meda Land LLC is a bulletproof hosting company that's become a powerhouse in the cybercriminal underworld. The service is run by Ukrainian Alexander Alexandrovich Volosovik (aka Yalishanda), who in July 2019, Brian Krebs named one of the most prolific bulletproof hosters in the world.

Volosovik, who touts his company on cybercrime forums, advertises its ability to host all manner of illicit sites and infrastructure. RiskIQ analysis shows that Media Land is also a driving force in the Magecart ecosystem. Magecart groups use Media Land-registered domains to carry out a massive amount of skimming and phishing attacks.

Media Land appears to be so ubiquitous that it rears its head in Magecart infrastructure even when it's not directly hosting a skimming domain, possibly used to bolster credibility among cybercriminals.

Our researchers have tied together significant swaths of Magecart infrastructure linked to the name 'Julio Jaime.' The name was first publicly documented by a Sucuri report from August of 2019, which noted Julio Jaime's use of 'Media Lend, LLC,' a name evoking the infamous service provider as the registrant organization on some WHOIS records. RiskIQ connects Media Lend, LLC to 180 malicious domains.

Julio Jaimes owns two email addresses that also include 'Media Land.' Together, medialand.regru@gmail[.]com and medialand.webnic@gmail[.]com have been used to register thousands of domains created for skimming and phishing. RiskIQ has tied the latter, medialand.webnic@gmail.com, to at least 98 domains, including several Magecart skimming domains.

The former, medialand.regru@gmail[.]com, appears to be unknown to the threat intelligence community until now. We used our Internet Intelligence Graph to connect the Magecart domains registered by these emails to several skimmers. Since December of 2018, RiskIQ has observed this email address used to register over 1,000 domains intended or actively used for skimming, phishing, and other malicious activities.

What's in a Name?

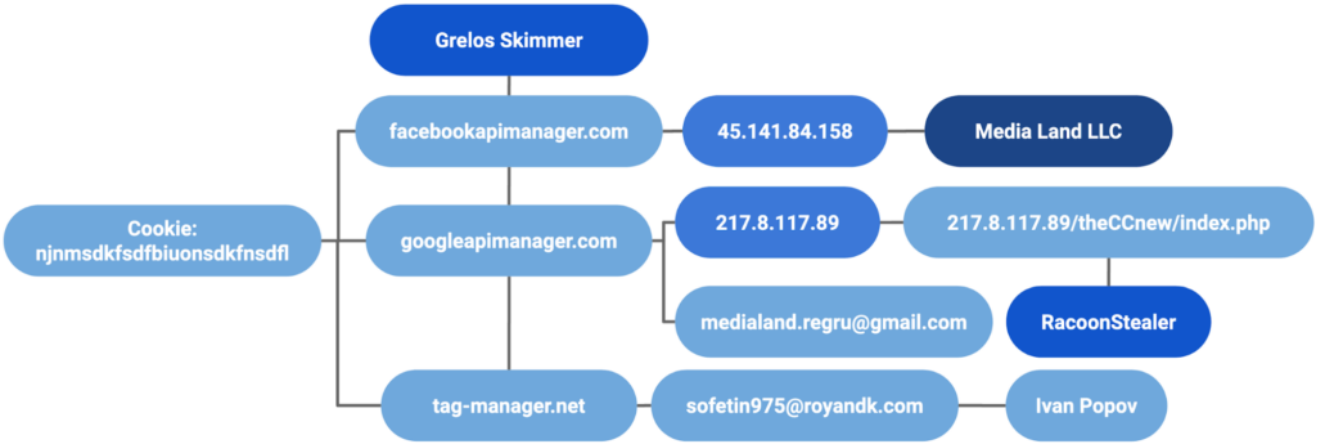
RiskIQ's Internet Intelligence Graph connects 'Julio Jaime' to more than 240 domains, most of which they developed for phishing attacks targeting end-users of financial institutions, such as the Bank of Ireland, and users of various services, such as Microsoft O365. These also include domains RiskIQ has flagged for hosting Magecart card skimmers. You can see two examples, cdnpack[.]net and gstaticapi[.]com in RiskIQ Community.

Julio Jaime also links to Magecart activity previously reported by RiskIQ. One of the domains tied to the email address medialand.webnic@gmail.com includes jquerycloud[.]com. Our December analysis of the Meyhod skimmer shows that our systems observed it on jquerycloud[.]com.

The domain jquerycloud[.]com was hosted on the same IP address as another domain, statexplore[.]com. On November 27, 2020, the WHOIS record for statexplore[.]com changed to use the email address medialand.webnic@gmail.com with the name Mihael Smith (an apparent misspelling of Michael) in lieu of 'Julio Jaime.' In our Inter Skimmer Kit post from September 2020, we noted similar use of random names for registrations, which is common among Magecart operators. However, in RiskIQ data, this misspelled name only associates with the two ‘Media Land’ email address covered in this report.

More Magecart Ties

In our November analysis on new variants of the Grelos skimmer, we highlighted the domain facebookapimanager[.]com and connected it to several other Magecart domains with a distinct cookie. Via the cookie, we connected facebookapimanager[.]com to another domain, googleapimanager[.]com, which was registered by medialand.regru@gmail[.]com, the email address belonging to the threat actor behind 'Julio Jaime' and 'Mihael Smith.'



Visualization of Magecart infrastructure connectivity

Googleapimanager[.]com was also linked to RacoonStealer info stealer via a shared IP address, which RiskIQ systems saw dropped from 217.8.117[.]89/theCCnew/index.php via our Crowdstrike intelligence integration. According to Ben Cohen at CyberArk, "Racoon is used to steal sensitive and confidential information including login credentials, credit card information, cryptocurrency wallets and browser information…" and is often delivered through phishing campaigns or exploit kits.

Scale your Defense in Response

Magecart attacks have skyrocketed, with RiskIQ detecting new attacks every few minutes. With more and more researchers looking into this growing threat, the massive scope of Magecart's cybercrime empire and its mind-boggling intricacies is finally being exposed. In response, organizations must have the intelligence necessary to scale their defense to meet this growing threat and be aware of how Magecart affects its attack surface.

From just two email addresses, RiskIQ's Internet Intelligence Graph was able to unearth large swaths of Magecart infrastructure and connect them to other activity, a key capability in protecting your organization from this top web-based threat. Be sure to check-in on RiskIQ's Threat Intelligence portal as we continue to track Magecart and publish the intelligence that can help you defend your organization. For the full report and full analysis, including IOCs, visit the intelligence card here.

Subscribe to Our Newsletter

Subscribe to the RiskIQ newsletter to stay up-to-date on our latest content, headlines, research, events, and more.

Base Editor