Lil' skimmer, the Magecart impersonator

blog.malwarebytes.com/cybercrime/2021/06/lil-skimmer-the-magecart-impersonator/

Threat Intelligence Team June 28, 2021

This blog post was authored by Jérôme Segura

A very common practice among criminals consists of mimicking legitimate infrastructure when registering new domain names. This is very true for Magecart threat actors who love to impersonate Google, jQuery and many other popular brands.

In this post we look at a skimmer recently disclosed by security researchers that has been around for over a year but managed to keep a low profile. In addition to naming several of their domains after Google, the threat actor is also naming their domains after the websites they have compromised.

Often, identifying additional infrastructure on the same network is a relatively simple exercize. But in this case it is more complex because the hosting servers are comprised of a large number of domains names, many of which are also malicious but not skimming related. Hiding in the noise is another common trait for threat actors.

Keeping it simple

This skimmer was publicly mentioned by Eric Brandel in early June 2021 and unlike Magecart JavaScript code, this one is very straightforward. Jordan Herman had also previously spotted this skimmer and referred to it as Lil' Skim. Based on an urlscan.io crawl, it appears the earliest instance is from at least March 2020, via googie[.]host.

> Newish Google themed digital skimming/#magecart domains
>
> googie-analitycs.site
> googie-analytics.online
> googie-analytics.website
> googletagsmanager.website
>
> Example on @urlscanio
> //googie-analytics.online/js/analytics.jshttps://t.co/wJMx4qP1z3
>
> Very simple/clean code: pic.twitter.com/L6QuU6ImJR
>
> — Eric Brandel (@AffableKraut) June 1, 2021

A dense network hiding more skimmer domains

A quick review of the Autonomous System (AS198610 Beget) where those skimmer domains are found shows a significant number of malicious hosts tied to phishing kits, Windows payloads, and Android malware just to name a few. Two IP addresses in particular, 87.236.16[.]107 and 87.236.16[.]10, are host to additional skimmer domains belonging to Lil' Skim.

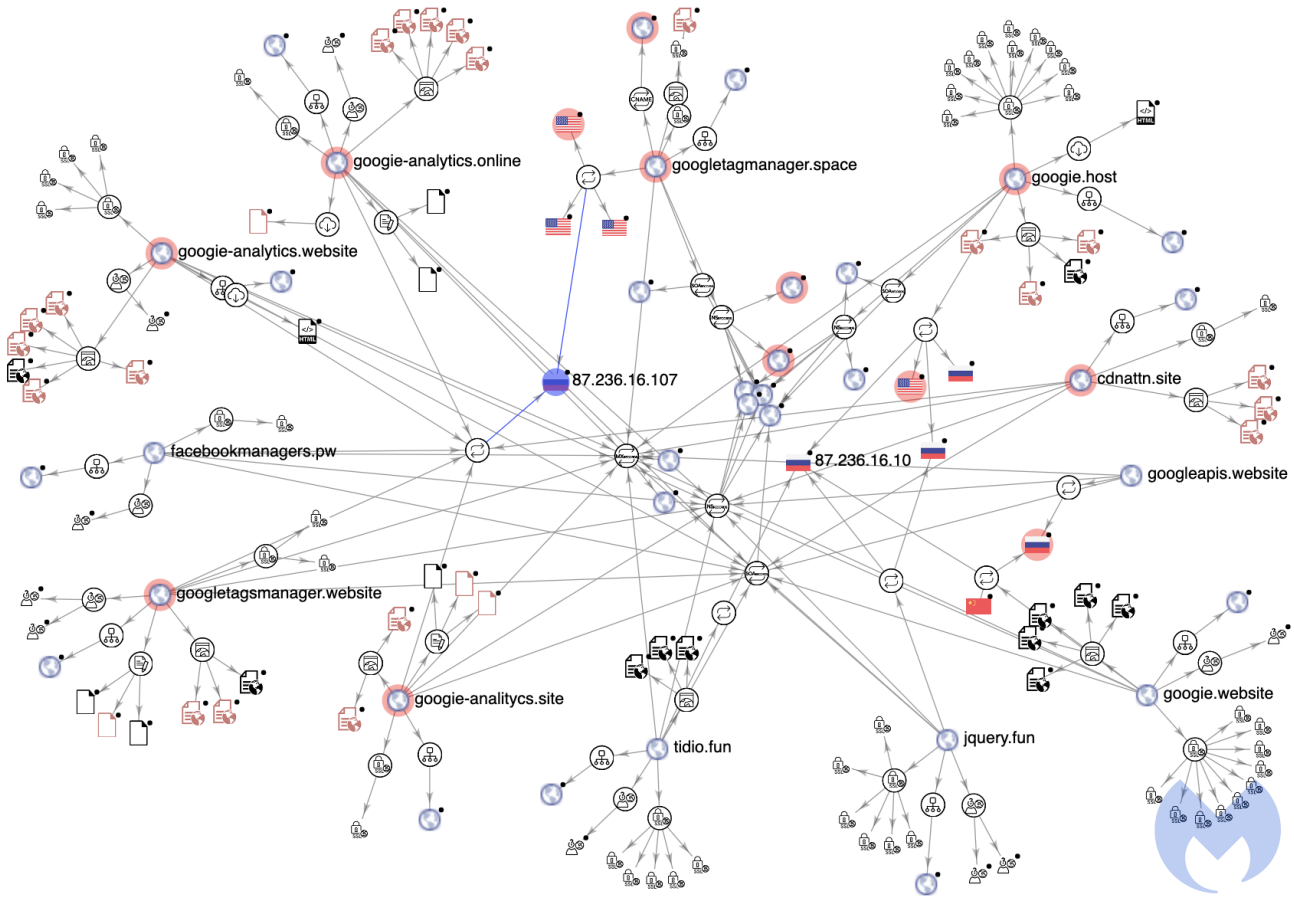

Figure 1: VirusTotal Graph showing a number of Google-like domains

For example, tidio[.]fun is a play on tidio.com, a chat application for website owners wishing to interact with customers. We recognize the same Lil' Skim code here as well:

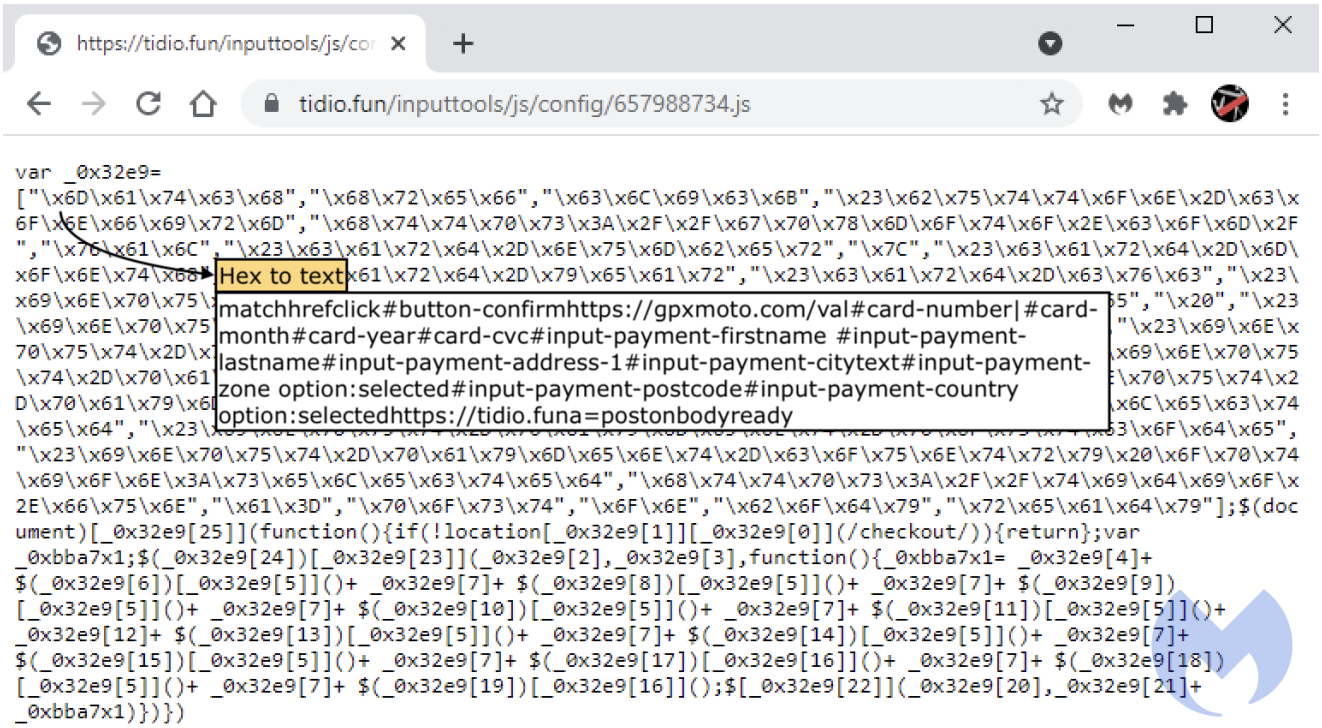

Figure 2: tidio[.]fun hosts the same Lil' Skim skimmer

Custom domains by compromised store

And then we discovered a number of skimmer domains that were named after compromised stores. This in itself is not a new practice and is often seen with phishing sites. The threat actor simply replaced the top level domain name with .site, .website or .pw to create hosts that load the skimmer code and receive stolen credit card data.

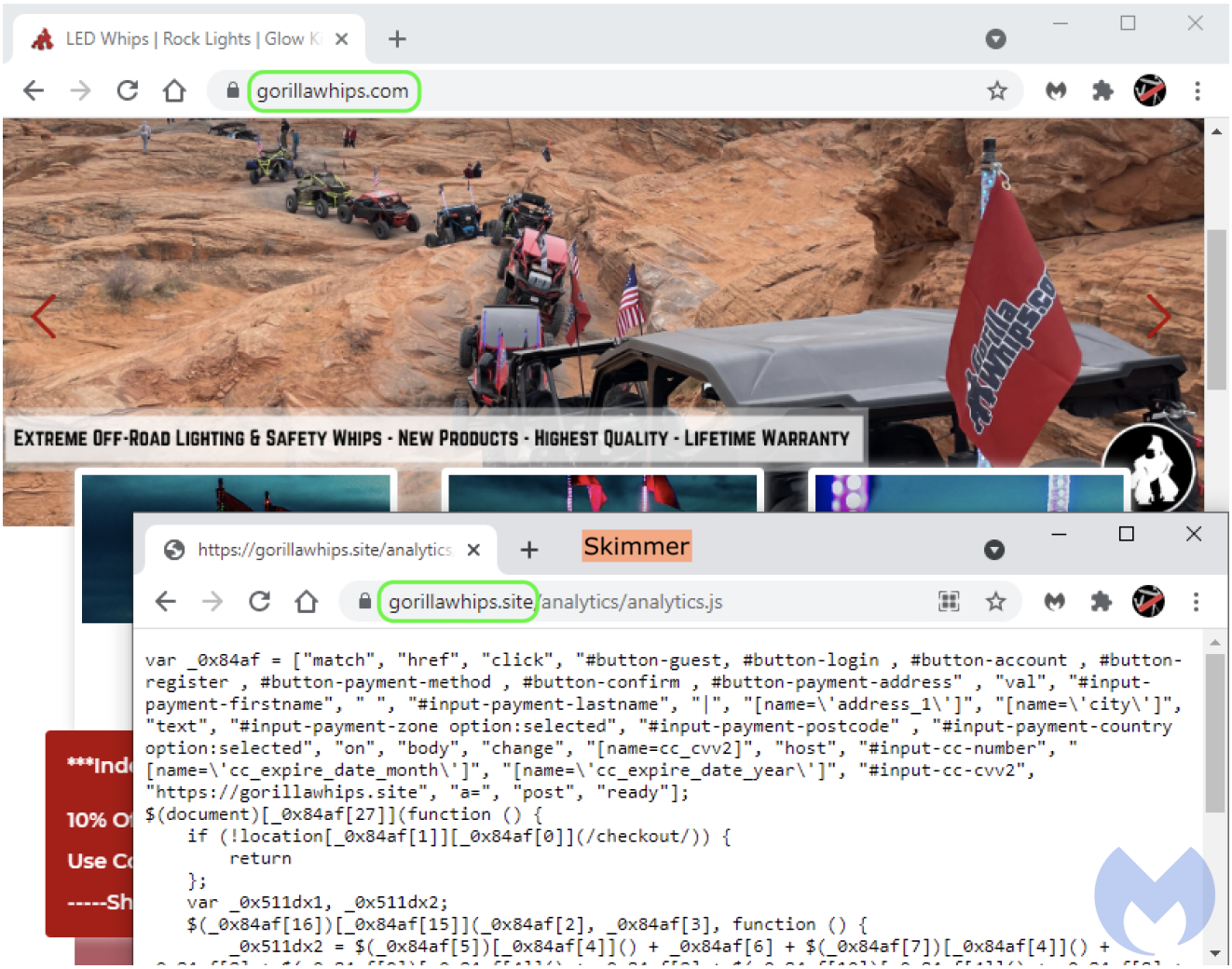

Figure 3: Legitimate website and copycat domain hosting a skimmer

Figure 4: Legitimate website and copycat domain hosting a skimmer
All the domains we found (c.f. IOCs) were hosted on 87.236.16[.]107.

Conclusion

Lil' Skim is a simple web skimmer that is fairly easy to identify and differs from other Magecart scripts. The threat actor is keen of impersonating internet companies but also the victim sites it goes after.

We were able to track this actor across the same ASN where they registered a number of different domains over a period of at least a year. There likely are more pieces of infrastructure to uncover here, but that might be a time consuming process.

We have notified the stores that have been impacted by this campaign. Additionally, Malwarebytes customers are already protected via our web protection module across our different products including Malwarebytes Browser Guard.

Indicators of Compromise

The following IOCs are linked to urlscan.io crawls whenever possible.

Standard skimmer domains

googletagsmanager[.]website
googie-analitycs[.]site
googie-analytics[.]online
googie-analytics[.]website
cdnattn[.]site
facebookmanagers[.]pw
googletagmanager[.]space
googie[.]website
googleapis[.]website
googie[.]host
tidio[.]fun
jquery[.]fun
cloudfiare[.]site

Skimmer domains impersonating compromised sites

perfecttux[.]site
gorillawhips[.]site
bebedepotplus[.]site
postguard[.]website
dirsalonfurniture[.]site
dogdug[.]website
bebedepotplus[.]website
perfecttux[.]website

Skimmer IPs

Known victim sites