# Webinject Panel Administration: A Vantage Point into Multiple Threat Actor Campaigns

team-cymru.com/blog/2021/11/03/webinject-panel-administration-a-vantage-point-into-multiple-threat-actor-campaigns/

S2 Research Team View all posts by S2 Research Team November 3, 2021

**The contents of this blog were shared with Team Cymru's community partners in the first half of 2021 and were subsequently presented by our analysts at RISE Las Vegas (September 2021).**

Much has been written about the role of webinjects in the evolution of banking trojans, facilitating the interception and manipulation of victim connections to the customer portals of a burgeoning list of targets which now includes e-commerce, retail, and telecommunications brands.

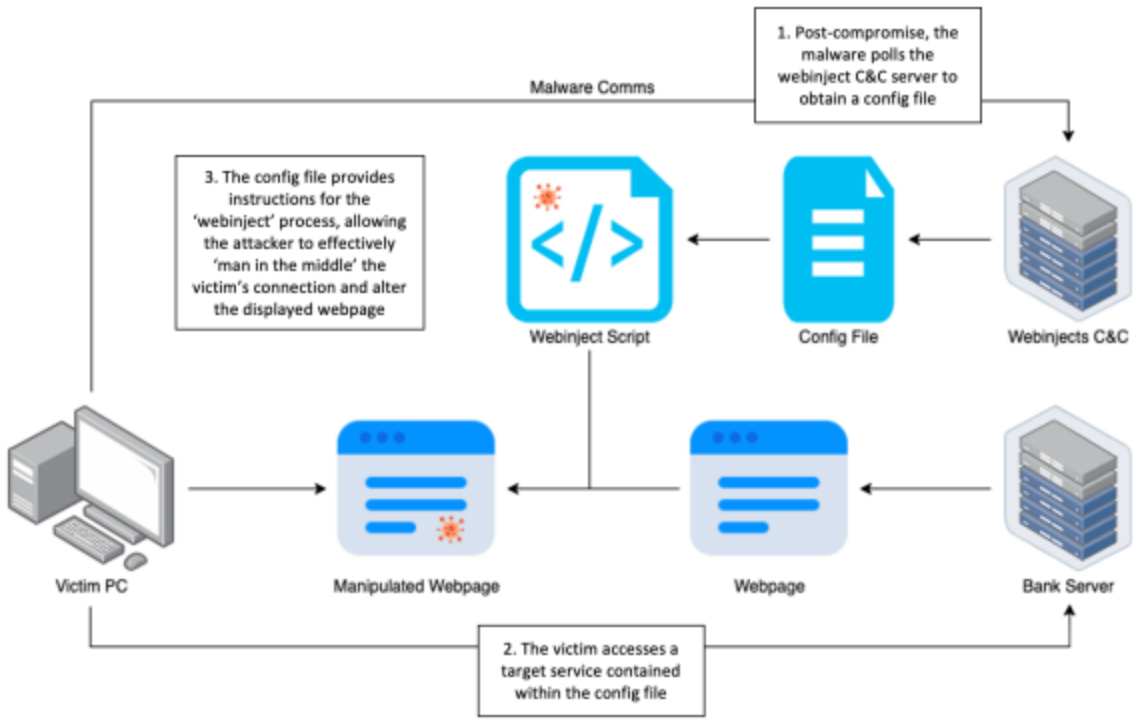


*Figure 1 – An overview of the webinject process*

Previous community research has also the highlighted the emergence of third-party webinject panel "providers" within the underground economy. For example, the moniker Yummba has long been associated with the creation/maintenance of webinject panels favored by many of the most ubiquitous banking trojan families, including IcedID, QakBot and ZLoader.

In this blog we will explain how we were able to track webinject infrastructure used by multiple threat actors over a period of more than six months. Using the concept of 'Threat Reconnaissance' to stay ahead of new campaigns, we were able to identify panels as they were set up and therefore limit their impact on potential victims.

## agentsjs[.]com

During investigations into IcedID (see our previous blog Tracking BokBot (a.k.a. IcedID) Infrastructure for further insights) in late 2020, a webinject panel used by the threat actors was identified hosted on **agentsjs[.]com**. A domain which at the time, based on Passive DNS information, resolved to **193.34.166[.]57** (assigned to SNEL, NL).

Whilst examining traffic to **193.34.166[.]57**, UDP connections with **95.213.129[.]178** (assigned to SELECTEL, RU) were identified using symmetrical source/destination ports – consistently UDP/23985.

Pivoting to look at traffic associated with **95.213.129[.]178**, further connections involving UDP/23985 were identified with fifteen other IP addresses within the 193.34.166.0/23 netblock. This activity was most recently observed on 9th January 2021.

**95.213.129[.]178** was also observed connecting to the above referenced IP addresses on TCP/22 and TCP/443 – activity likely related to the setup and management of the panels.

Passive DNS information was used to enrich these IP addresses, as summarized in Table 1.

| IP Address | Domain |
|---|---|
| 193.34.166[.]17 | knockdout[.]com |
| 193.34.166[.]172 | batchjs[.]com |
| 193.34.166[.]210 | toughjs[.]com |
| 193.34.166[.]241 | queryfrm[.]com |
| 193.34.166[.]243 | minifyscss[.]com |
| 193.34.166[.]246 | authdetect[.]com |
| 193.34.166[.]36 | entryquery[.]com |
| 193.34.166[.]87 | navsjs[.]com |
| 193.34.167[.]109 | wellsoffice[.]net |
| 193.34.167[.]116 | acceptjs[.]com |
| 193.34.167[.]198 | authfw[.]com |

| | |
|---|---|
| 193.34.167[.]209 | intellix[.]site |
| 193.34.167[.]227 | cdnreact[.]com |
| 193.34.167[.]248 | huntinqton[.]net |
| 193.34.167[.]94 | onedrive-registration[.]com |

*Table 1: IP addresses in communication with 95.213.129[.]178*

Through our botnet analysis efforts, we were able to link several of the domains contained in Table 1 to webinject panels attributable to specific threat actor groups; Dridex, IcedID and QakBot.

Our initial assessment of these findings was that **95.213.129[.]178** was being used as some form of management channel for these panels and given the attributions to multiple distinct campaigns, likely associated with a third-party webinject vendor.

However, from 10 January 2021 onwards, we did not observe any further communications of note involving this IP address.

### 31.131.249[.]98

We continued to monitor traffic associated with the 193.34.166.0/23 netblock, looking for similar UDP connections to known / unknown panels.

Commencing on 18 January 2021, we noticed connections involving **31.131.249[.]98** (also assigned to SELECTEL, RU) with a handful of 'new' IP addresses. These connections similarly used symmetrical ports – in this case consistently UDP/23743.

Between 18 January and 24 May 2021, we identified ten additional panels based on connections with **31.131.249[.]98**. Of note was the apparent re-use of **193.34.167[.]248** (see Table 1) which had hosted **huntinqton[.]net** in November 2020 and then reappeared in March 2021 hosting **outresult[.]com**.

As was the case with **95.213.129[.]178**, **31.131.249[.]98** was also further observed connecting to the above referenced IP addresses on TCP/22 and TCP/443.

As previously, passive DNS information was used to enrich these IP addresses (Table 2).

| IP Address | Domain |
|---|---|
| 193.34.166[.]159 | widgetcdn[.]com |
| 193.34.166[.]223 | tagscdn[.]com |

| | |
|---|---|
| 193.34.166[.]27 | typescdn[.]com |
| 193.34.166[.]98 | fetchjs[.]com |
| 193.34.167[.]145 | bacassets[.]com |
| 193.34.167[.]200 | servjs[.]com |
| 193.34.167[.]203 | toughjs[.]com |
| 193.34.167[.]24 | procjs[.]com |
| 193.34.167[.]248 | outresult[.]com |
| 193.34.167[.]52 | authframework[.]com |

*Table 2: IP addresses in communication with 31.131.249[.]98*

We were able to link several of the domains contained in Table 2 to webinject panels associated with IcedID and QakBot campaigns.

### Passive DNS

Given the apparent concentration of webinject panels hosted within the 193.34.166.0/23 netblock, as well as some apparent commonalities in domain naming convention:

- frequent references to ‘cdn’ or ‘js’
- references to terms associated with content and website delivery, e.g., ‘auth’, ‘fetch’, ‘query’, and ‘tags’
- some targeting of specific financial entities, e.g., ‘huntinqton’ and ‘wellsoffice’

We decided to review passive DNS data for the entire netblock.

From a total of over 1,000 domains, a further 17 were highlighted as likely relevant to this analysis (Table 3).

| IP Address | Domain |
|---|---|
| 193.34.166[.]12 | backedjs[.]com |
| 193.34.166[.]217 | minifycdn[.]com |
| 193.34.166[.]230 | querymask[.]com |
| 193.34.166[.]35 | elementquery[.]com |
| 193.34.166[.]42 | jqrequire[.]com |
| 193.34.166[.]55 | jquerylibs[.]com |

| | |
|---|---|
| 193.34.166[.]8 | purejscdn[.]com |
| 193.34.167[.]120 | interqu[.]com |
| 193.34.167[.]134 | requiredjs[.]com |
| 193.34.167[.]229 | projectsjs[.]com |
| 193.34.167[.]237 | jqueryslib[.]com |
| 193.34.167[.]25 | statecdn[.]com |
| 193.34.167[.]35 | requirejscdn[.]com |
| 193.34.167[.]41 | jscdn[.]cyou |
| 193.34.167[.]65 | widgetcdn[.]com |
| 193.34.167[.]72 | sublimejs[.]com |
| 193.34.167[.]89 | zefjs[.]com |

*Table 3: Webinject panels hosted in 193.34.166.0/23*

As previously, we were able to link several of the domains contained in Table 3 to webinject panels associated with Dridex, IcedID and QakBot campaigns, additionally one of the domains was linked to ZLoader.

## Conclusion

By identifying the upstream IP addresses described above and subsequently monitoring traffic, we were able to observe threat actor infrastructure being set up in the days and hours before it was used to target victims. This allowed us to work with our community partners to limit the impact on potential victims.

The concept of ‘Threat Reconnaissance’ that we seek to promote using our Pure Signal™ Recon platform, is the idea of proactively tracking threat actors so that Threat Intelligence becomes more than just a reactionary function.

By focusing on the webinjects element of the banking trojan attack model, we were able to apply this idea to multiple threat actor groups within the same reporting strand.

We hope that this research adds to the collective understanding of webinject panels, in particular how they are managed and distributed within the underground economy. Figure 2 (below) illustrates our understanding of how the operation described in this blog takes place.

***Note that Figure 2 makes specific reference to 193.34.167[.]248 which, as previously mentioned, was used to host two webinject panels and was observed in connections with both 95.213.129[.]178 and 31.131.249[.]98.***

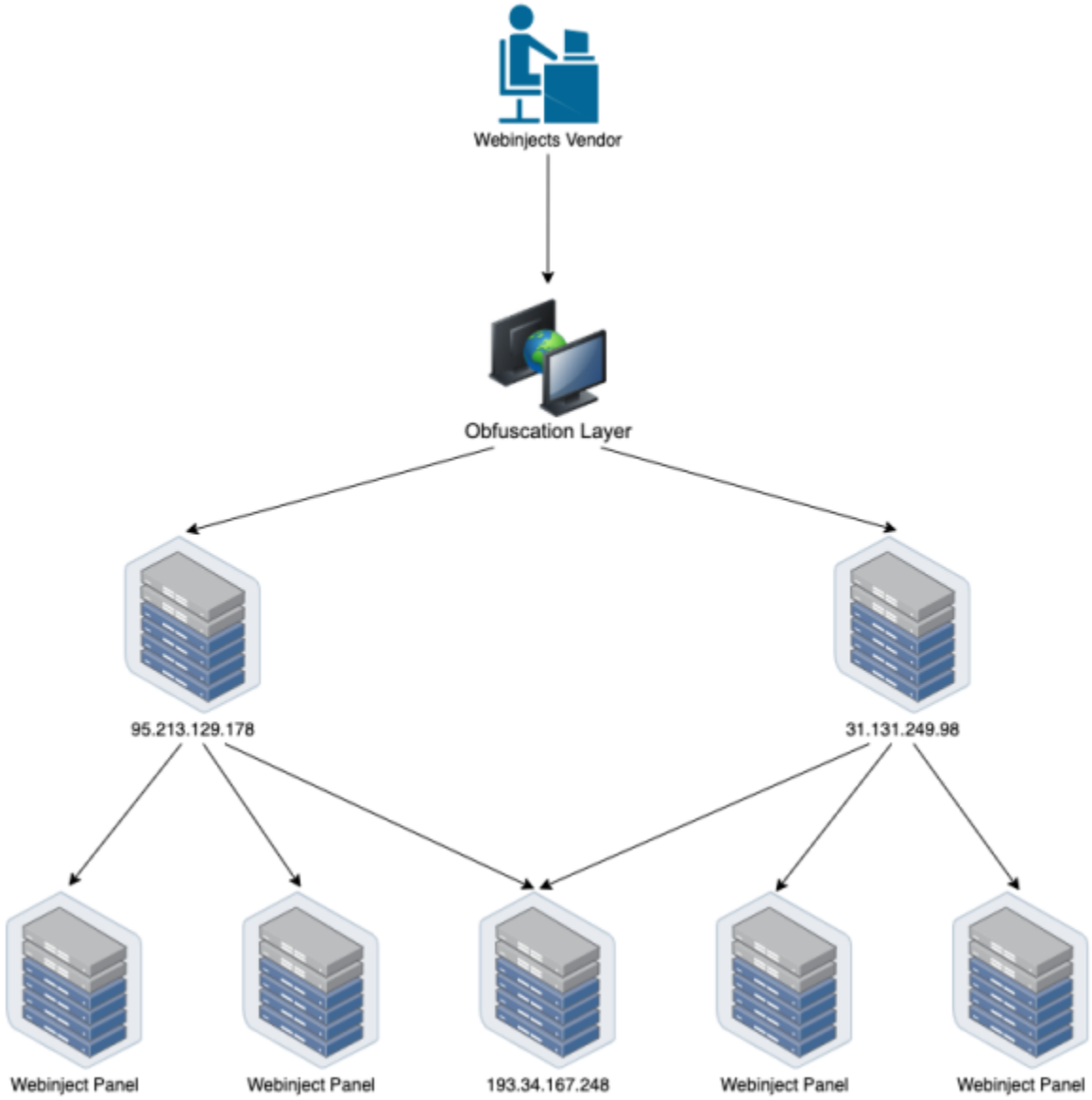


*Figure 2 – An overview of the identified infrastructure*