# Pivoting: finding malware domains without seeing malicious activity

silentpush.com/blog/pivoting-finding-malware-domains-without-seeing-malicious-activity

May 28, 2019

May 28
Written By Ken Bagnall

First Published February 1st 2021 by Martijn

**It is part of the job of a threat actor to ensure the domains used in their campaigns blend in with the crowd and stay undetected for the duration of the campaign. It is part of the job of an analyst to spot such domains by looking for ways in which they still stand out.**

While looking through Silent Push's trove of data, I spotted the domain cdn12-web-security[.]com. At first glance, this domain looks like a normal domain, part of the content delivery network of a web security service. However, it is slightly odd that more than three months after the domain was registered, cdn*n*-web-security[.]com doesn't exist for any other *n*.

We have also learned to be a bit suspicious of these very normal looking domains: the main domain used in the SolarWinds supply-chain attack, avsvmcloud[.]com, remained undetected for months at least in part because it looks so very normal, seeming to belong to an AWS-like cloud service and hardly standing out among the domains you'll see in your DNS logs.

On top of this, in the past month alone, we have seen cdn12-web-security[.]com point to no fewer than six different IP addresses in succession, which is fairly unusual:

80.249.147[.]241
47.91.92[.]75
80.249.147[.]144
47.254.131[.]6
8.208.87[.]225
8.208.101[.]136

Still, we have not seen any malicious activity linked to the domain. In fact, there does not appear to be any public activity linked to the domain at all, which suggests that whatever it

is that the owners of the domain are doing, they keep it small enough to stay under the radar.

But let us look at the IP addresses. Two of them (80.249.147[.]241 and 80.249.147[.]144) belong to Russian hosting provider Selectel in Russia, while the other four belong to Alibaba's US operations. In Silent Push's systems, these two ASNs have fairly high (i.e. bad) IP reputation scores (35 and 28 respectively), which suggests a fair number of malicious URLs hosted there. It should be noted though this isn't too uncommon for large cloud provider: Amazon AWS's IP reputation score currently stands at 19.

Now let us look at the IP address to which the domain pointed to during the last week of January, 8.208.101[.]136, and see what else is hosted there.

During the last week in January, the domain secure-dns-resolve[.]com also pointed to this IP address. And for this domain we have public activity of both malware connecting to it and a phishing image hosted there. Interestingly, and almost certainly not coincidentally, was saw this domain point to the same six IP addresses throughout January, going through them in the same order.

Another domain name pointing to the same IP address is dns16-microsoft-health[.]com. Here too we find public evidence of malware that has connected to it. It will not surprise anyone that dns*n*-microsoft-health.com doesn't exist for any other *n*. The domain has also cycled through the same set of IP addresses we saw before.

This is also true for a fourth domain we saw pointing to 8.208.101[.]136 recently: cdn12-show-content[.]com. Here though we find no public evidence for activity linked to this domain, malicious or not.

**Still, given the many similarities, we are confident to say cdn12-web-security[.]com and cdn12-show-content[.]com are operated by the same actors who also operate secure-dns-resolve[.]com and dns16-microsoft-health[.]com and should be blocked just as much. The same is true for a fifth domain, ms-health-monitor[.]com, which has been linked to malware and which was taken down in January.**

Another thing that links these five domains is the use of DNSPod's name servers, which have a not too great reputation of 18 in Silent Push's systems.

**These five domains aren't the only ones linked to the mentioned IP addresses. For example, righttime4mercy[.]com currently points to 80.249.147[.]144; this domain has been linked to a Hancitor malspam campaign in the past.**

It may thus be that behind these IP addresses are managed by a bulletproof hosting provider which rents out its infrastructure to malicious actors and shields them from takedown requests. The Hancitor domain may thus be unrelated to the other five, though of course no less malicious.

## Conclusion

Pivoting around an IP address or a domain name isn't generally a very reliable way to link malicious activity, given the wide use of shared and compromised infrastructure, as well as the use of false flags by more advanced actors. However, it should not be totally ignored either.

We started from a single interesting looking domain for which no malicious activity could be found. Through the Silent Push API and with the help of a few search engine searches, we were able to link it to an active malware campaign, and possibly found part of a bulletproof hosting operation.

Ken Bagnall