Revealing REvil Ransomware With DomainTools and Maltego

domaintools.com/resources/blog/revealing-revil-ransomware-with-domaintools-and-maltego

Looking at a Recent REvil (AKA Sodinokibi) Ransomware Indicator Set in Maltego Using the DomainTools Transforms

According to a recent report by Symantec Enterprise Security, the REvil ransomware operators have been seen leveraging Cobalt Strike and scanning for vulnerable Point-of-Sale systems. The attackers are utilizing a mixture of AWS CloudFront for C2 and Pastebin for storing their payloads. Leveraging legitimate services here makes it difficult for incident responders to react as any number of things may rapidly shift as infrastructure can be quickly spun up, torn down, and modified on cloud services with a host of modern configuration management tooling. However, the report included three IP addresses that can be investigated to provide more insight. With ransomware on the rise again, it’s important to do proper due diligence to see what else one can discover behind this single instance. I’ll do so by leveraging the DomainTools data set and Maltego to visually map out my research.

First, the domains and IP addresses released in the report were:

102.129.224[.]148

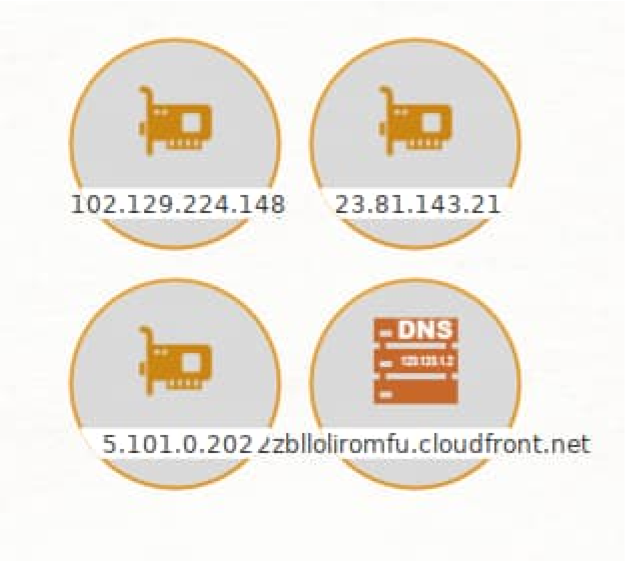
23.81.143[.]21
5.101.0[.]202
d2zblloliromfu.cloudfront[.]net

Although not directly mentioned in the report, it is helpful to time gate when this attack occurred to limit the scope of research. Since cloud services can shift at any moment (and indeed that CloudFront address for instance has had hundreds of allocations since January 2020), placing a barrier around the research will help separate signals from noise. As this report was released in late June 2020, I'm going to assume that the attacks took place after April of 2020. The reason I'm choosing this date is due to a bit of domain knowledge as a security professional: there are multiple reports that came out during the height of COVID-19 that indicated the group behind REvil were leveraging COVID-19-themed lures and attacking medical infrastructure with great effect. I can make an educated guess that at least one associate has shifted their targets now that the effectiveness of those lures is drying up.

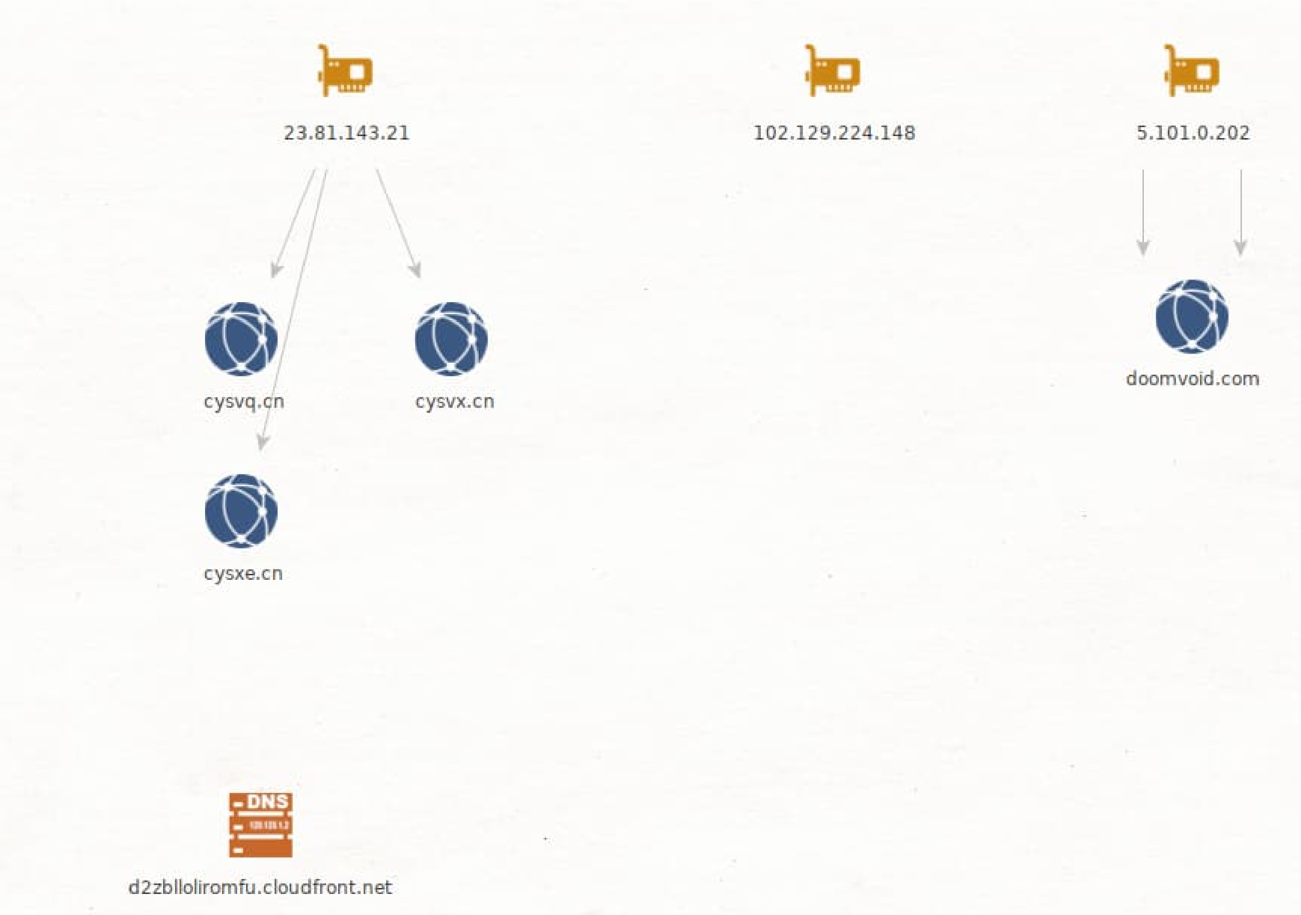
An additional note before I begin: REvil samples usually contain thousands of domains used for C2, many unregistered and suspected decoys. The group is advanced in that there are a swath of methods used for exploiting victims and moving laterally in victim's networks with more than a dozen tools used to do so. They adapt their techniques for each organization they attack and evolve with each unique campaign. If you are looking to track REvil beyond understanding a single campaign event then I would suggest reading KPN's excellent write-up on tracking the group across hundreds of individual campaigns. If you are looking for a write-up of how a singular sample works I cannot recommend McAfee's analysis enough.

Investigating with Iris and Maltego

So to start, I'll import these four entities from the report into Maltego. The paste function does a good job here of figuring out what types of entities these are.

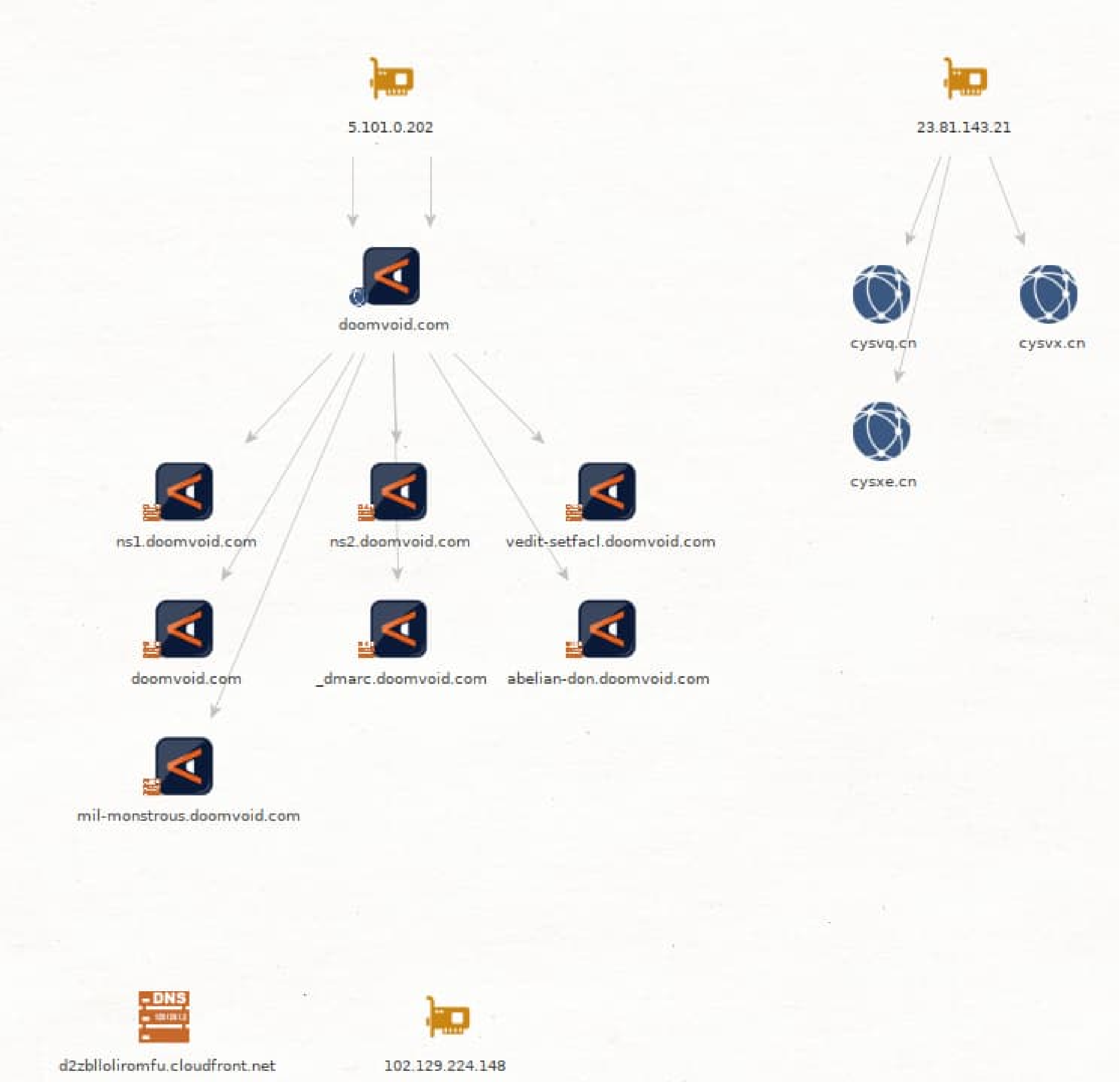


From there I’ll run a reverse lookup, marked under the DomainTools Iris transforms as “IP Address to Domain” to get several domains to begin our searching.

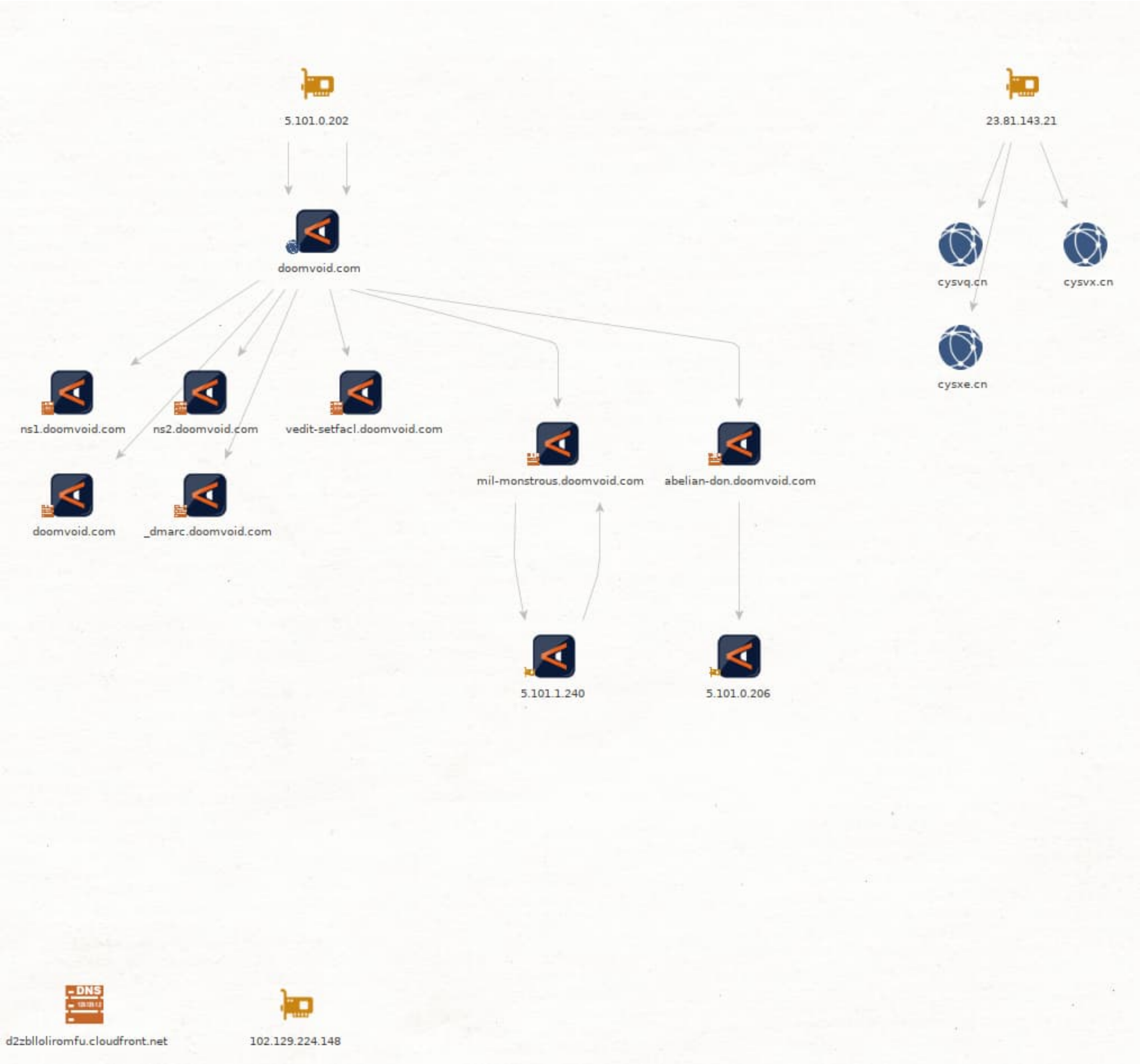


From a quick look at the entity details brought in from the Iris transforms I noticed that the domains in the CN TLD are all from 2016 and before. Since I’m time gating our investigation I’ll take a look at just the doomvoid[.]com domain then. Running that through the Farsight

Passive DNS transform, I get a number of suspicious domains that fall within the time constraints.



The fact that this domain is running its own nameservers is suspicious enough with how often nameservers are now used for C2 signaling. The vedit-setfacl is interesting as that references in setfacl a Linux command used to set file access control lists and seems an odd error or perhaps a command mistype that ended up being picked up by a recursive resolver's passive DNS sensor. Outside of those, both the abelian-don and mil-monstrous subdomains seem the most suspicious. Polling Farsight again for A records linked to those subdomains, I get two new IP addresses for this investigation.



Out of those two new addresses, the only one that returns any additional context in our time frame is the 5[.]101[.]0[.]206 address which I can pull a domain vila[.]website from using the Iris Investigate transform once again. This site, registered in May of 2020 through reg.ru had a DomainTools Risk score of 93 out of 99 with a high chance of malware. This algorithm takes into account nearby domains, infrastructure this domain sits on, and its history to determine the likelihood of its potential for maliciousness. 93 is considered a very high likelihood from the DomainTools machine learning classifiers. This may be in part due to the IP addresses associated existing on the Petersburg Internet Network, a Russia-based ISP located in Saint Petersburg from which malicious traffic has been observed in the past. Knowing that the REvil group is suspected to be Russia based, the high likelihood of malicious traffic from this network, and our timeframe I can do a search for all Farsight Passive DNS query sets in that time frame for a[.]vila[.]website and I’ll get back four IPs in total.

5.8.54[.]52
5.101.0[.]206
5.8.55[.]43
5.101.6[.]227

From here, outside of these IP addresses being on the same network as our original indicators, unfortunately, I cannot do much more to tie these to additional indicators or past reports. From this point, I can see that all of the IPs were likely linked during the same timeframe, but all there is left to do is monitor for maliciousness.

With each REvil associate and attack being well contained and with some instances being hosted on constantly shifting cloud infrastructure it’s important to become adept at mapping out an attack as quickly as possible in some visual form that can be passed along to leadership. Leveraging Maltego, the Iris Investigate transform, and other transforms at my disposal I can rapidly build out a report in Maltego for export.

Learn more about streamlined incident response with DomainTools and Maltego:

Learn More