High Value Malicious Domains.

silentpush.com/blog/high-value-malicious-domains

May 28, 2019

May 28
Written By Ken Bagnall

First Published Dec 18th 2020 by Ken

Malicious domains vary enormously in quality depending on the use case and the expected lifespan of the proposed campaign. For example if someone was running a phishing campaign and wanted to fool a user into clicking a link, the domain used for the link may not even matter if it is masked in the email and the user is going to believe they are clicking on something else in the HTML. A low value malicious domain is likely to be used in this scenario. This could involve something as easy as registering a subdomain similar to the intended victim as part of a dynamic domain service such as noip.org. An example of these recently around would be.

hxxps://voicenett.serveftp[.]com/6s17aiqf1hczfv7e

These don't necessarily need to survive for very long depending on what the next stage of the planned attack is and can be redirected to any desired payload.

Next in the stack would be similar domains to the victim or the victims supply chain. These can work very well particularly for email campaigns.

Some recent examples from threat feeds would be

Level 2

loop.microsoftmse[.]com

wellsconfirm-account[.]com

aliorbank[.]io

The use case may this time be to put in the reply-to field of an email as an example. Business Email Compromise would be a typical example. Its a little more visible to the victim and therefore needs to be convincing.

On the next tier would be domains that stand out by themselves and look like they would provide a valid service. These are getting into the high value territory now as there may not be an obvious reason to block them. They don't look like another domain to be caught by a typo squatting rule and may not look anomalous in network traffic, or the service copied is very generic like Microsoft. However the use case is different to those mentioned before as it may not be email related.

Level 3

microsoftupdateswin[.]com

serviceupdates[.]net

servicesupdater[.]com

These are very convincing and can be used for long standing campaigns and may survive for a period of time. This also results in these domains being recycled and reused over the years, even if they have previously been taken down after being discovered being involved in malicious activity.

Differentiating after this is broken down into tactics and procedures of the attacker and things get quite difficult. In order not to give away too much of the defenders toolkit I won't go into further detail on this.

Examples From UNC2452 also known as Dark Halo/Sunburst

So now to the indicators from the recent breaches that have been revealed so far.

Nearly all the domains fit into the level 3 category and some would fit into a category higher due to associated tactics. Firstly they used one main domain which was critical to their campaign.

Avsvmcloud[.]com

This was further broken down into various subdomains using a Domain Generation Algorithm. Some good work was done on uncovering the links to victim names here.

This primary domain had its own Nameserver which only had one domain on it.

"domain": "avsvmcloud[.]com",

"to_ns_srv_domain_density": {

"a1-139.avsvmcloud[.]com": 1,

"a11-64.avsvmcloud[.]com": 1,

"a20-65.avsvmcloud[.]com": 1,

"a26-67.avsvmcloud[.]com": 1,

"a4-65.avsvmcloud[.]com": 1,

"a6-66.avsvmcloud[.]com": 1

The domain switched to using this name server on 27th February 2020 around the time the attack began

The list of Nameserver changes for this domain is here

NS Changes. 2

"date": 20191207,

"days_ago": 374,

"domain": "avsvmcloud[.]com",

"from_nameservers": [

"ns1.dnsowl.com",

"ns2.dnsowl.com",

"ns3.dnsowl.com"

"to_nameservers": [

"pdns09.domaincontrol.com",

"pdns10.domaincontrol.com"

"date": 20200227,

"days_ago": 292,

"domain": "avsvmcloud.]com",

"to_ns_srv_domain_density": {

"a1-139.avsvmcloud.com": 1,

"a11-64.avsvmcloud.com": 1,

"a20-65.avsvmcloud.com": 1,

"a26-67.avsvmcloud.com": 1,

"a4-65.avsvmcloud.com": 1,

"a6-66.avsvmcloud.com": 1

There are a few notable details here. Switching of name servers just before a campaign signifies a management process around attacker infrastructure and that is the case for most of the domains in this campaign. Therefore we give these types of domains a higher category of “Managed High Value Malicious Domains” In our API for our Threat Intelligence enrichment we capture this concept with the field of NameServer Entropy.

The rest of the domains have a similar profile except they use a shared NameServer.

Domain

Avsvmcloud[.]com

Freescanonline[.]com

Zupertech[.]com

Panhardware[.]com

Databasegalore[.]com

Incomeupdate[.]com

Highdatabase[.]com

Websitetheme[.]com

Thedoccloud[.]com

Virtualdataserver[.]com

Lcomputers[.]com

Webcodez[.]com

deftsecurity[.]com

digitalcollege[.]org

globalnetworkissues[.]com

kubecloud[.]com

seobundlekit[.]com

solartrackingsystem[.]net

virtualwebdata[.]com

To push this idea to the next stage is to see if you can evolve this profile and use it to hunt for more similar domains and see if this technique is more widespread.

Creating a query to look for similar profiles to the main domain which had to operate from its own nameserver may lead to other instances of actors using the same technique.

This leads us to a list of very useful domains that have been registered in a similar pattern as the original avsvmcloud[.]com. This does not mean these are in any way malicious, just worthy of a further look.

Updates[.]run

fedora-dns-update[.]com was associated with APT22 (Suckfly)back between 2014-2016 but unknown now

virtualserverfaq[.]com

microsoftsonline[.]net -which has already been identified in a different breach claimed to be APT41

microlynconline[.]com -which has already been identified in a different breach claimed to be APT27

The list is much longer but very much speculation, so we won't list any more in a public forum. Threat Hunters can use this profiling methodology to query datasets such as from Silent Push to draw a list of candidates worthy of monitoring. Keeping an internal Passive DNS service going on your own organizational traffic and hunting on all newly encountered domains within that to correlate with the list of profiled domains would also be worth doing.

Another useful piece of information that surfaces from this is that it is worthwhile searching within the vast volume of threat indicators you receive for "High Value Domains" and treating them differently. We have made this available in the advanced filtering part of the Threat Intelligence Analysts interface.

Our Silent Push enrichment service is now available to Beta customers and those on our customer advisory board. If you would like to join us building out this service to suit your requirements please join our Beta program

Name *
Thank you!

Ken Bagnall