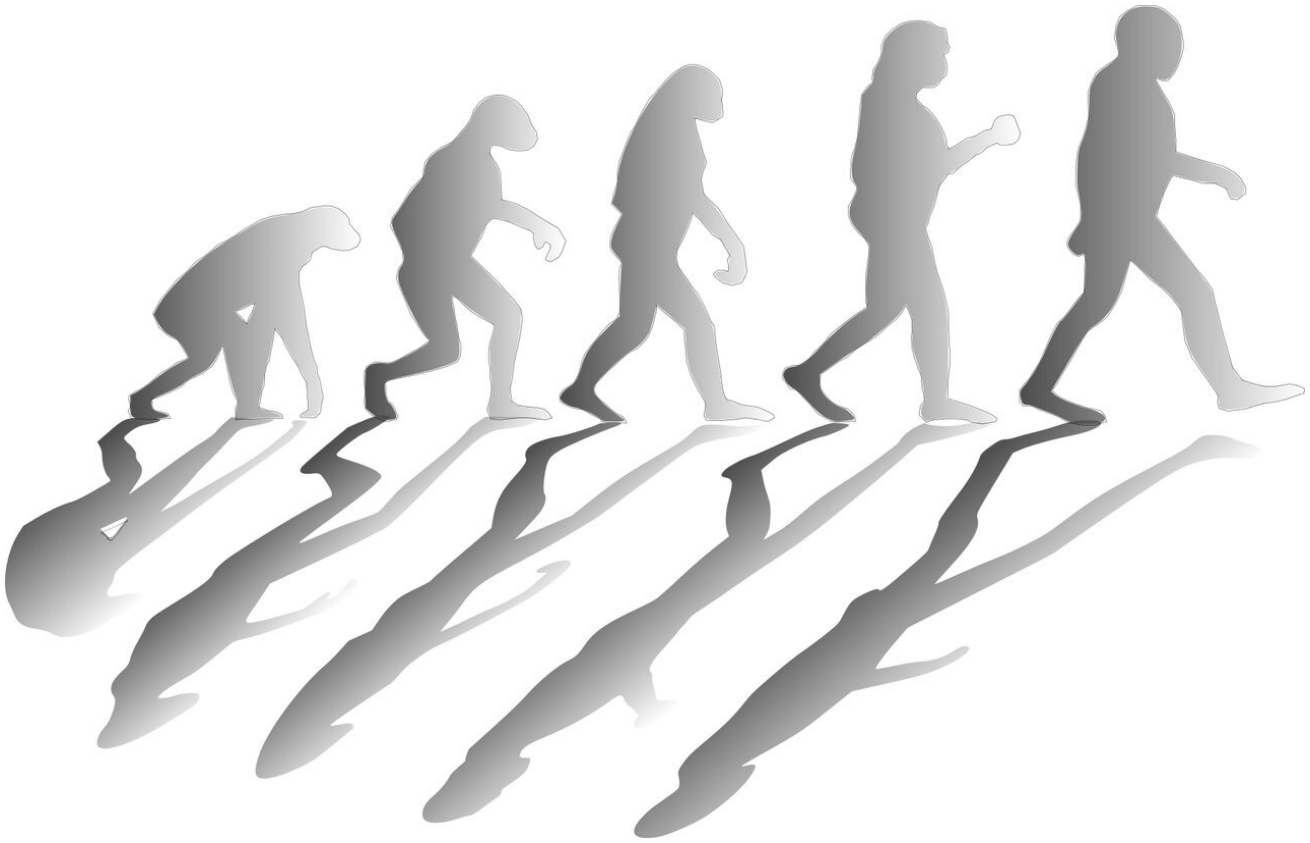
Investigating Crimeware Name Servers

silentpush.com/blog/evolution-cyber-attack

May 28, 2019

May 28
Written By Ken Bagnall



First Posted December 21st 2020 by Ken

Very few security products and services give enough consideration to the reputation and quality of the Name Server associated with domains they are looking at. We pick here a High Value Suspicious Domain and check what else is on the same name server to examine what is discovered through the process.

Our seeding domain will be service-update[.]link
Looking at the Name Server info from our API

"domain": "service-update[.]link",

"ns_avg_ttl": 4149,

"ns_domain": "dendrite.network",

"num_domains": 203,

This is a low density Name server where we have only seen 203 domains on it. It has a very low average TTL across all the domains on there which may suggest a lot of changes compared to other name servers.

A quick lookup using our explore API gives us a number of suspicious domains with matching characteristics. These appear to be in two groups.

Group 1.

Commonalities- Tech related theme. Nameserver domain- dendrite.network. Have an A record-AS holder ColoCrossing- Registrar Namesilo- "address": "Tavernier St., Wall House",

"city": "Loubiere",

"country": "DM",

Domain PTR Record Potential Target Registrar

update-support[.]network *colocrossing.com 3 Mobile UK Namesilo

service-update[.]link *colocrossing.com Live soon Namesilo

hs-securealerts[.]com *colocrossing.com HSBC Namesilo

ref0948a[.]com *colocrossing.com unknown Namesilo

uk-taxupdate[.]com *colocrossing.com HMRC Namesilo

aem-new[.]com *colocrossing.com 3 Mobile UK Namesilo

aempath[.]com *colocrossing.com 3 Mobile UK Namesilo

com-gb[.]mobi *colocrossing.com Mobile UK Namesilo

It appears that Group 1 have either been used maliciously already or are waiting to be used maliciously. Monitoring the “waiting” group for changes is key as this may lead to being able to block their activity once the domain moves into an actively malicious mode. There are a number of ways to do this such as monitoring for new changes in DNS or associated records. Moving of infrastructure can often mark an activation of a malicious domain. A good example of this is when the domain avsvmcloud[.]com was activated for the Solarwinds breach, it switched to its own nameservers for the active part of the campaign.

Group 2.

This group seems to lead to more and more indicators so I’ll post them over time.

Commonalities- Tech related theme. Nameserver domain- dendrite.network. Domains have been aged. Have an A record-AS holder Nice IT Services Group Inc.

- Registrar Namesilo- "address": "Tavernier St., Wall House",

"city": "Loubiere""country": "DM

Domain AS Name of IP Potential Target Registrar

Paypalservice[.]support Nice IT Services Paypal Namesilo

small-url[.]cc Nice IT Services adobe and others Namesilo

election[.]finance Nice IT Services malware download Namesilo

Ulsterbankonlineltd[.]com Nice IT Services Ulster Bank(RBS) Namesilo

Choicebank[.]online Nice IT Services Choice Bank/First Choice Namesilo

Documentcloud[.]pw Nice IT Services adobe and others Namesilo

rbscotland-online[.]com Nice IT Services Royal Bank of Scotland Namesilo

Btctools[.]net Nice IT Services Bitcoin Wallet stealer Namesilo

gb-kpmg[.]com Nice IT Services KPMG Namesilo

secure-id[.]cloud Nice IT Services Secure ID Namesilo

service-ca-verification[.]com Nice IT Services Flagged as spammer Namesilo

Teamtnt[.]red Nice IT Services Malware Downloads Namesilo

So just touching on these two groups based on similarities, these of course could be one group, this Nameserver is very heavily used by malicious actors and definitely one threat actor group called Team TNT.

How can I use this information?

All the information above was collected by our API and can be leveraged for threat hunting or detections. The information is pre-collected and cached so new lookups don't have to be done each time you have a new indicator to check. We've already collected all this information and run some analysis on it to give things like reputation scores for the nameserver, the AS number reputation, the subnet reputation etc.

A security team can use Yara rules over this information to try and find "High Value Malicious Domains " in their logs or associated IP addresses.

We also have threat hunting API endpoints that gather behavioral clusters for you so you can quickly create your own new intelligence, or we can do it for you.

Name *
Thank you!

Ken Bagnall