CYBER STASH

How To Defent Against COVID-19 Centered Cyber Threats Using Actionable Threat Intelligence

eclipse

Executive Summary

Between February and March of this year, CyberStash saw an increase in blocked network connections per day from 185 million to 221 million. This represents an alarming 20% increase in one month. If this trend continues, the total number of network connections blocked by the CyberStash Cyber Threat Intelligence Gateway will increase by over 1.5 billion or 30% from February levels. Over 50% of these network connections are being blocked as a result of threat intelligence blacklists and over 40% of connections are being blocked based on GEO-IP policies.

DomainTools, one of our strategic threat intelligence partners, recently made available a free, curated list of high-risk COVID-19-related domains. This is an admirable move by DomainTools and their desire “to support the community during the Coronavirus crisis.”

As a service to our customers and consistent with our vision of making threat intelligence actionable, we have quickly moved to integrate this threat intelligence into the CyberStash Cyber Threat Intelligence Gateway.

In this article we will look at:

- *DomainTools COVID-19 threat intelligence findings*
- *DomainTools COVID-19 Threat List*
- *How you can use threat intelligence to improve network protection and visibility into COVID-19-related threats.*

Observations

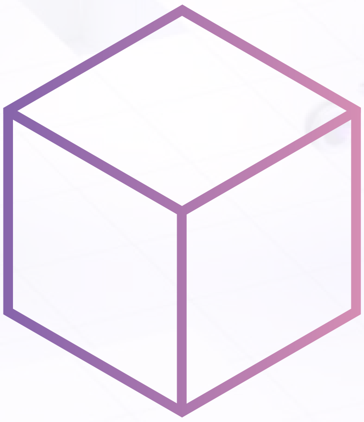
The increased volume of blocked network connections that we are observing is being driven by three specific factors:

1. Increased network traffic as organisations scramble to open their networks to a significant, unexpected increase in remote users;

2. Greater threat volumes with opportunistic threat actors taking advantage of the Coronavirus pandemic

3. Tighter policy controls as customers look to improve network defenses and reduce risks amidst an expanded attack surface.

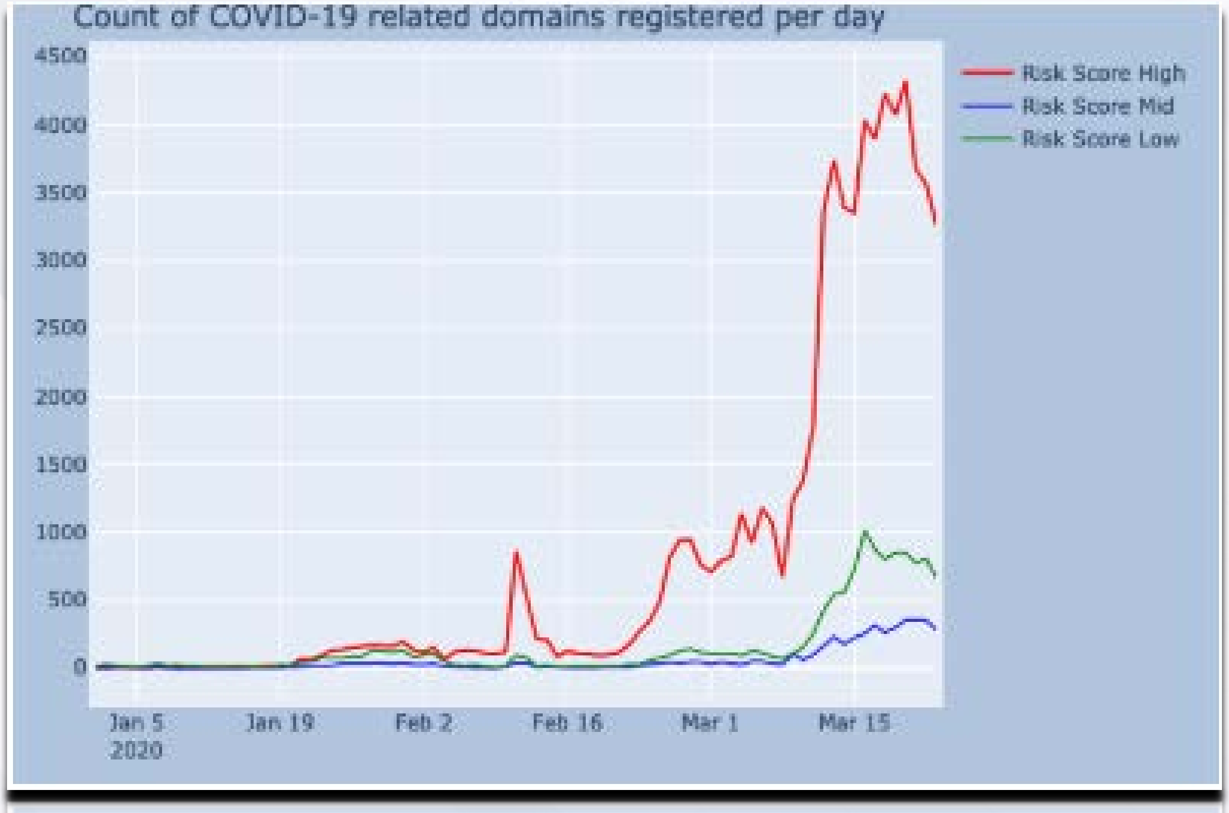
Threat actors are taking advantage of the COVID-19 pandemic to launch cyberattacks, including phishing campaigns. This is validated by data from DomainTools which shows a significant increase in domain name registrations per day relatedto COVID-19 terms.



Registered COVID-19 Related Domains Per Day

The figure below shows a massive uptick in domain registrations that started March 14, with more than 3,500 new domains being registered daily thereafter.

While recent data shows a decline in the volume of daily registrations from peak levels, they remain at elevated levels. According to DomainTools, the list has proven to be quite volatile and immediately responsive to changing news regarding COVID-19.



COVID-19 Threat List Details

In order to identify and categorise threat intelligence specifically related to COVID-19, DomainTools took into account four distinct considerations:

List Criteria

- Domains registered on or after January 1, 2020
- Domain names containing one or more terms or term variants related to COVID-19
- Domains having a Domain Risk Score of 70 or higher

Terms and Variants

- DomainTools generated a list of terms identified and being used in malicious domains related to COVID-19. Some examples include “corona”, “covid19”, and “chineseflu”. They then ran these terms through their PhishEye algorithm to generate potential “phishy” variants of these terms. Some examples of these variants include “c0vid”, “corrona”, and “koronawirus”.

- DomainTools is actively monitoring the terms used for this list compared to new domain registrations and will make changes and updates to the list over time as needed.

COVID-19 Threat List Details

Risk Score

- The DomainTools Risk Score enables a determination of the perceived level of risk associated with listed domains. The COVID-19 Threat List is sorted by both risk score and domain create date. Domains are scored on a 0 to 99 scale, and DomainTools by default recommends that scores of 70 and higher are indications that the domain was registered with malicious intent.

- Note that this DomainTools COVID-19 threat list is considered “predictive” as many of these domains are not yet operationalised. As such there are not specific indicators of compromise for these domains. Therefore, DomainTools recommend users consider this threat list as a “watchlist for future positives.”

Using COVID-19 Threat Intelligence in the CyberStash Cyber Threat Intelligence Gateway

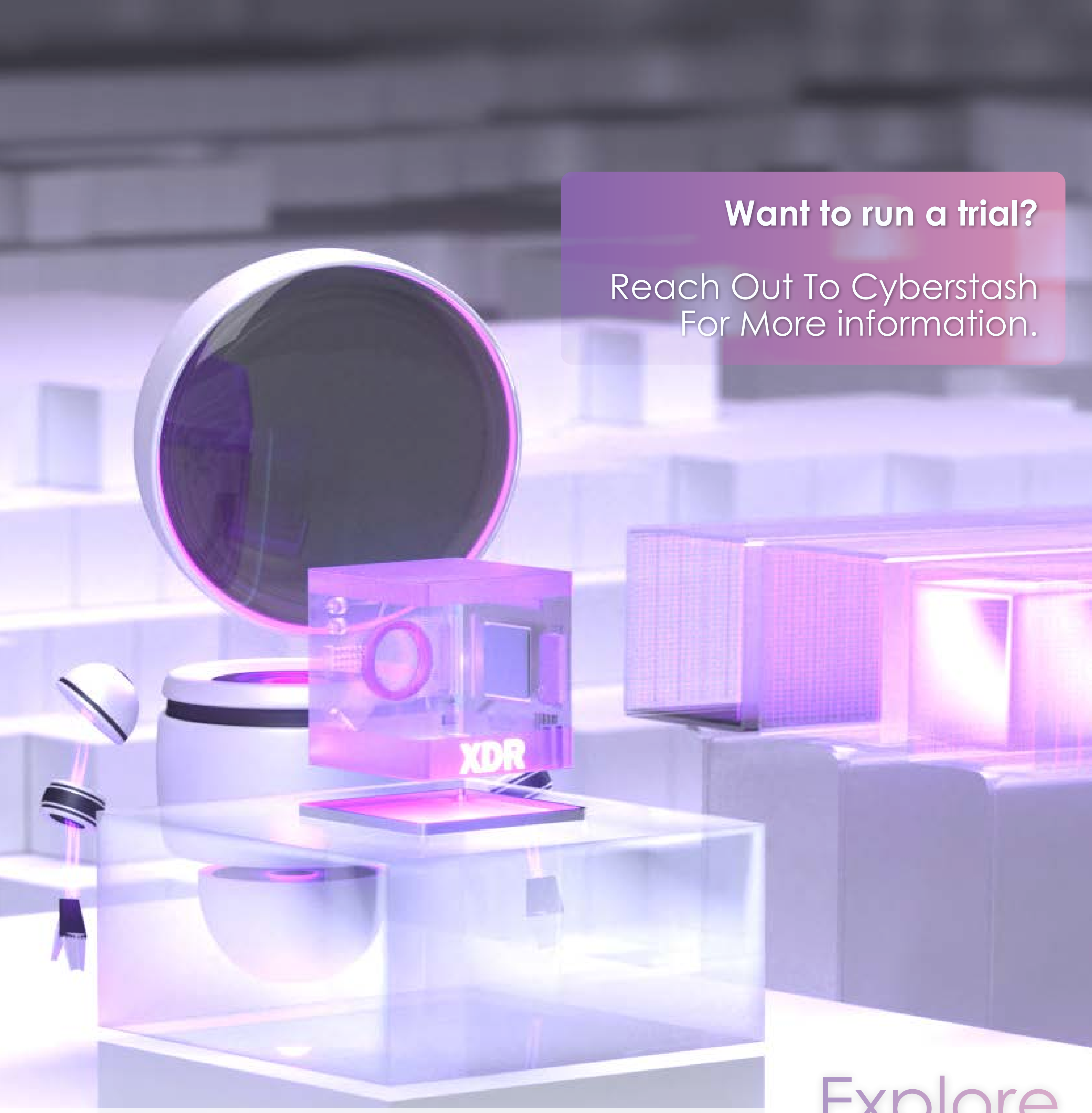
Consistent with our mission of making threat intelligence actionable, we've made the DomainTools' COVID-19 threat intelligence available to all CyberStash customers. Specifically, we've made available two automatic domain blacklists.

Terms and Variants

1. COVID-19-DomainTools-99 is a list of COVID-19-related domains with a Risk Score of 99 and higher. This list currently contains over 50,000 domains and represents a very high to definite level of confidence that the domain is malicious.

2. COVID-19-DomainTools-70 is a list of COVID-19-related domains with a Risk Score of 70 and higher. This list currently contains over 90,000 domains and represents a medium to high level of confidence that the domain is malicious.

We recommend that customers treat the blacklist with Risk Scores of 99 and higher as a blacklist and treat the broader list with Risk Scores of 70 and higher as more of a "watch" list.



Want to run a trial?

Reach Out To Cyberstash
For More information.

Explore
eclipse.xdr

info@cyberstash.com
1300 893 802
cyberstash.com
Sydney, Australia

CYBER STASH