athena dynamics

Defending Against the Undetectable via Detectionless Technologies

Author: Ken Soh, Group CIO, BH Global and CEO, Athena Dynamics
Copyright © Mar 2020 All Rights Reserved Athena Dynamics Pte Ltd

---

Executive Summary

This paper focuses on the common yet long-neglected pitfall of today's cyber protection technologies. It addresses the fundamentals why incidents continue to happen despite substantial investment into cyber protection.

To address such pitfall, detectionless technology of "Content Dis-arm Reconstruction (CDR)" or "Content Deconstruction, Neutralization and Reconstruction (CDNR)" technology is discussed. The paper also provides concise and important verification guideline to help readers identify a true CDR/CDNR tool from many that claim to be one.

Why do we continue to make the same mistake?

Today, advanced threats are not detectable. Unfortunately, security leadership continues to focus only on detection centric technologies. Be it multi-AV, sandboxing, machine-learning, threat-intelligence etc, they are all working on the same fundamental of "exploiting the most advanced technologies to detect the bad in order to remove the bad". Such paradigm works but is dangerously inadequate for the basic reason that we cannot detect many of the advanced threats in the first place. Even if they are detected today, it cannot be done so tomorrow. We cannot be focusing on running a never-ending catch-up game.

Why is detection-only mindset so dangerous?

Detection-only mindset provides a dangerously false sense of security. "We have deployed the most marketed, most well-known world-class cyber security protection technologies and we are now safe". For security leaders who protect with such mindset, not only that there is no 100% security, mostly likely the "most well-known world-class" technologies are detection centric. It is important to have detection centric protection. However, it is dangerously incomplete without complementing it with detectionless technologies.

ATHENA DYNAMICS PTE LTD
8 Penjuru Lane, Singapore 609189.
Tel: 65 6291 4444 Fax: 65 6291 5777
www.athenadynamics.com

So, what do we mean by "detectionless technologies"?

Detectionless technology is a broad term that I use to describe any technology that does not protect by *"sensing out the bad"*. In many occasions when I mention that we protect detectionlessly, I am likely be mistaken by "ah certainly, you are referring to pre-empted, pro-active prevention". Many do not get the point the first time. I typically need to educate them that I am not referring to "protection by prevention only". We *prevent detectionlessly*. Unfortunately, from experience, this concept typically takes time to share and educate. This could be due to the fact that the detection oriented mindset is deeply ingrained in most peoples' minds all this while.

Detectionless Protection as an Ongoing Pursuit

As mentioned earlier, detectionless is a broad term of our focused pursuit thus far. It entails technologies that focus on neutralization, isolation and specific peripheral technologies that augment the detectionless approach when it falls short. We reckon that the quest for "detectionless" is never a destination but an ongoing journey, since new, disruptive approaches emerge from time to time. It is the nature of technology development. In this article, we would like to introduce a selection of such technologies as general references.

"CDR" vs "CDNR" and why "Neutralization"?

Some call it Content Dis-arm and Reconstruction (CDR), we prefer to call it Content Deconstruction, Neutralization and Reconstruction (CDNR). We have published a separate paper on this which is available via *this link*. Simply, we felt that the word "Dis-arm" infers detection, and since the technology does not involve detection, CDNR would be a more accurate articulation of this technology in our opinion. This way, the essence and beauty of detection-less paradigm would stand-out naturally.

Specifically, with reference to dictionary.com, to neutralize something means to make it neutral or harmless. Neutralization is the name of this process. If you help defuse a bomb, you contribute to its neutralization. This would be a great term than some other commonly used ones such as "scrubbing", "sanitizing", "flattening" etc.

Detectionless via Neutralization

What do we mean by Neutralization? In lay-man's words, we do not "detect", just "detox". There are too many examples that detection-based parameter defences would screen and approve incoming traffic for users positively, only ending up users being attacked by advanced threats via such "approved clean traffic" eventually. We cannot detect advanced threats. Detect nothing does not mean it is safe in today's threat landscape.

So what do we do via Neutralization? At file level, Neutralization re-constructs files via file conversation implemented as a highly scalable, enterprise cross-domain or e-mail platforms. At packet level, re-construction is implemented via packet conversion platform that accepts user-exits that interfaces with custom user-defined deconstruction and reconstruction routines. Both technologies have already protected numerous CIIs at classified and secret levels.

In a nutshell, Neutralization is a zero-trust, white-listing approach at its conceptual level. While it is difficult to identify the bad, we simply pick up the good since we know what are the good better than what are the bad. By simply removing the “bad’ or “impurities” regardless of whether it is malware, by sieving out only the required good that we know best, we achieve high level of protection since the impurities could be known or unknown malware, which could be zero-day viruses or even unborn viruses.

Finally, it is also important to understand that once the approach is detection centric, the subconscious thought is that the world is all good and hence the objective is to identify the bad. This has been proven ineffective needless to explain. Neutralization works on the concept that the world is bad and we simply pick up the good that we want, since we know that best. It is an implicit and indirect work of white listing.

Identifying a True CDR/CDNR Tool from the Claiming-to-be

While the market starts to understand the strength of CDR/CDNR just like decades ago when the term “Firewall” first emerged, it is also risky to choose a CDR/CDNR platform at face value. Now that CDR/CDNR has started to reach the peak of the technology hype curve, various propositions are starting to claim their availability of CDR/CDNR feature. How hence could we identify the real McCoy? For that, we would recommend some key identifying facts that end-users could reference in their procurement evaluation effort:

1 – Fidelity of neutralized files/packets

Every vendor would claim that they are the best. Use case oriented stress testing is therefore the most direct and useful approach to identify the “real McCoy”.

2 – How many file types does the solution support?

A matured CDR/CDNR product should support at least all common file types which would usually amount to around 100 types. It would be unfortunate to realize after deployment that the platform does not support certain file types needing to be neutralized.

3 – Track record

When did the product start to offer CDR capabilities? How many productive CIIs does the product protect till date? It is observed that some security products claim to have enhanced with CDR/CDNR capabilities. Deeper assessment based on this list is key.

4 – Is there deep CDR/CDNR at finer granularity of files and emails?
Many perform CDR/CDNR at just the file or email level. There is benchmark that proves multiple folds of efficacy of threat prevention to perform CDR/CDNR at finer granularity of file or email.

5 – Does the solution handle encrypted email attachment?
Encryption protects privacy for us for the longest time in the history of information sharing. Unfortunately, today, it also protects viruses. A well implemented CDR/CNDR enterprise platform should have matured process flow to handle and CDR/CNDR encrypted attachments., providing a good balance between security and productivity operationally.

6 – Does it support a highly scalable enterprise platform?
Since enterprise CDR/CDNR typically forms an integral part of businesses, it is important that it comes with highly scalable capability that allows scaling up and down without the need for down time.

7 – Does the vendor have credible, local presence?
Since CDR/CNDR will be an integral protection shield of the organization's crown jewel, it is important to verify that the supplier has a credible local presence for ongoing support requirements.

8 – Does it offer external connectors to other solutions in the workflow for situations when checking of executables are necessary? e.g. SCADA domain.
CDR/CNDR provides strong protection. Unfortunately, the technology by nature does not support executable binaries. The platform should therefore provide flexible SDK/API and connectors for customized workflow in use cases when executables needs to be shared.

Other Detectionless Technologies
CDR/CDNR is a strong and effective option to protect detectionlessly. There are other options such as Isolation and Containment (ISOC), Micro-Segmentation etc which are not the focus of this paper. We are happy to share more if there is specific interest to know more. Please feel free to contact us via contact@athenadynamics.com.

What Constitutes a Complete Cyber Protection Technology?
With the understanding of detection centric vs detectionless cyber protection paradigm, the typical technical strategy is therefore to complement detection-based hygiene level protection with detectionless innovations as per the following illustration. We do not oppose the use of detection technology. Detection operation typically saves time. However, since we cannot detect advanced threats in the first place, it is best to complement existing detection strategy with the detectionless technology to complete the loop.

In a nutshell, unlike the detection way which typically focuses on the hygiene level of protection and the cause of attack, detectionless way focuses on eradicating the undetectable at the source in a bid to eradicate the causes. Collectively, both approaches would provide a highly strengthened security posture.

How would the above Paradigm affect the Traditional Cyber Protection Strategy?
As per the above, we advocate strongly the combination of detection centric and detectionless technologies. However, cyber protection is not just about technology. It is the usual People, Process, Technology (or Platform) that cover the full spectrum of cyber protection considerations. We have only discussed about the Technology element in this paper. For the People and Process elements, we too have radically different views from the traditional approach. We are keen to explore separately with the reader should there be interest. These could be addressed separately since each of these element entails larger and deeper subject matters.

Source: https://athenadynamics.com/event/defending-undetectable-via-detectionless-technologies/

Disclaimer: The outcome of general best practices introduced in this material may vary due to environmental and contextual parameters. Neither BH Global Corporation Ltd, Athena Dynamics Pte Ltd nor the writers are responsible for any direct or indirect implications/impacts to the readers due to the adoption of these practices.

Not for Distribution. No part of this presentation materials may be distributed/reproduced without the writers' expressed consent.