SOLUTION BRIEF

NOT JUST A NUMBER:

Scoring the Risk of an IP Connecting to a Network

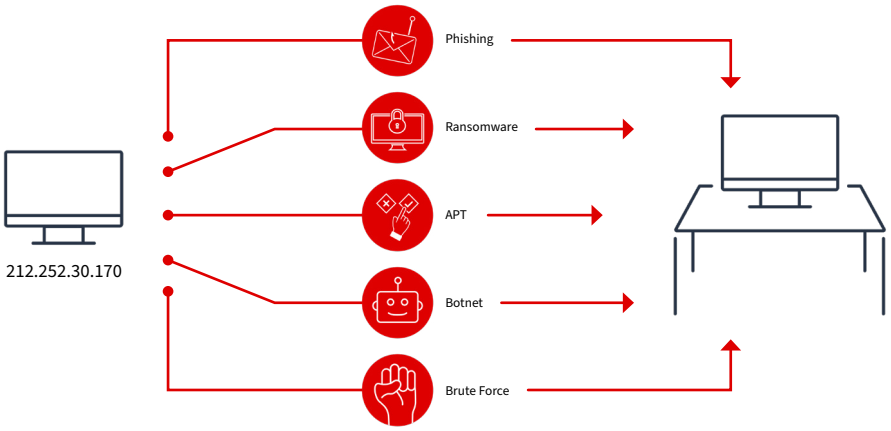
NETWORK DEFENDER

CELERIUM.com

NOT JUST A NUMBER:

SCORING THE RISK OF AN IP CONNECTING TO A NETWORK

In the ongoing and escalating battle between cybersecurity professionals and cyber criminals, the good guys enjoy one advantage: irrespective of the attack vector, methodology, objective, or its sophistication, every cyberattack must be launched from a computer with an IP address. The bad news is there are nearly four billion IP addresses in use today creating a noisy, confusing environment in which attackers can hide.



Large, well-funded organizations have teams of cybersecurity analysts that are focused on picking apart good network traffic from bad, identifying false positives, and tracking threat actors. This approach provides value because, as mentioned above, the unalterable reality of how the Internet works is that every attack must come from a source IP address to a destination IP address. This means cyberattacks can be detected or stopped by using IP addresses as the source of truth. Unfortunately, most firewalls can't support block lists that contain hundreds of thousands of bad IP addresses, so which ones do you block? There are plenty of threat intelligence offerings on the market today, but they can be expensive and require dedicated analysts to use. Even worse, both free and paid sources of threat intelligence have a challenge with "false positives," meaning something good got on the blocklist and if you block it, someone is going to get mad.

Celerium's Cyber Defense Network™(CDN) is different. We approach the challenge of detecting and blocking threats from a new perspective. Our solution is built from the ground up with a focus on supporting small and medium sized companies, or even highly distributed large enterprises that may not have the time, people, or money to adopt the traditional approach to security operations. Our approach prioritizes machine-to-machine communications, removing humans from the loop. We used data, analytics, and our hard-earned experience to design Network Defender® with a combination of three distinct, but complementary, automated approaches to identifying known or likely attacks to our customers' networks and stopping the attacker in their tracks.

"...irrespective of the attack vector, methodology, objective, or its sophistication, every cyberattack must be launched from a computer with an IP address."

GENERATING SCORES

Before we get into our scoring approaches, let us first talk about how and why we generate threat scores. Our customers stream real-time network traffic details to Celerium's CDN infrastructure using native capabilities that exist in most firewalls (e.g., syslog or netflow). We process all of that data in real- time using a highly scalable infrastructure that parses that stream of data into valuable metadata such as where the traffic came from, how much data was sent, and the technologies related to those communications (e.g. remote desktop or web traffic). To be clear, we never see the content of those communications. With every inbound or outbound network communication, we look at the IP addresses associated with those communications and send that to our automated scoring engine. This engine checks to see if we have a recent score generated for that IP address or not. If so, the score is used within CDN for a wide array of functions. If that IP has not been scored, or if it has been too long since we last scored the IP, we kick our automated analytics into gear using our proprietary "three-legged stool" of analytics. The three parts of this approach are named:

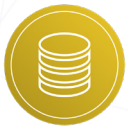
"If an IP has not been scored...we kick our automated analytics into gear using our proprietary 'three-legged stool' of analytics."

Signal-Based Intelligence

Predictive Analytics

Community Analytics

SIGNALS-BASED INTELLIGENCE



The first challenge to solve when providing fully automated scoring is how to process massive amounts of information from a wide array of sources to make a determination of how safe or dangerous an IP might be. To solve this problem, we created a new approach that we coined "Signals-Based Threat Intelligence." The idea behind this approach is to avoid thinking about the information collected from threat intelligence sources in terms of malware command and control, phishing, or ransomware hosts, but rather to treat the appearance of an IP on a threat intelligence source as a signal of bad activity. We can then look across time and across sources to determine how strong that signal might be at any moment in time. Signals can be weak or strong. The combination of signals and their strength affects our calculation of Threat Score. This table compares two Threat Score examples to illustrate how Signals-Based Intelligence generates a Threat Score.

"The first challenge to solve when providing fully- automated scoring is how to process massive amounts of information from a wide array of sources to make a determination of how safe or dangerous an IP might be."

	SCORE = 6	SCORE - 9
Number of Times Observed	Seen on 4 Lists	Seen on 2 Lists
Age of Target	3 months old in all 4 cases and is no longer on any of the 4 lists	New - IP address was added to both lists today
Quality of Lists	Low - Historically, the lists hve not been reliable indicators of compromise	High - Historically, the lists have been reliable indicators of compromise
Correlation of Lists	High - the same IP addresses appear on all lists	Low - the IP addresses do not appear on all lists

PREDICTIVE ANALYTICS

In some cases, the IP address or domain name we're scoring doesn't appear in our Threat Intelligence Library. However, our robust collection of threat intelligence sources allows us to use Predictive Analytics to determine if an IP address that is not in our Threat Intelligence Library shares attributes with risky IP addresses that are in our library; the number of shared attributes allows us to predict whether this IP address is likely to be malicious.

For example, if our platform is scoring an IP address that was registered yesterday with a less-than-reputable registrar in a nation known to be a source of malicious activity, and with a randomly-generated set of characters for a name, it will be scored as a high-risk IP even it it's not yet on any threat intelligence lists.

The 2017 WannaCry exploit provides a compelling example of how Celerium's Predictive Analytics can identify a malicious IP before it's highlighted as problematic on traditional threat intelligence lists. In its attack, the WannaCry perpetrators used a randomized domain name on their server, meaning the server used to launch the attack was named via a random string of characters, not a name that an organization would typically assign to a server used for legitimate purposes. Based on this and other criteria, Network Defender, using Predictive Analytics, assigned the domain name used in the WannaCry exploit with a Threat Score of 8 before that exploit was named or published by other organizations.

"The 2017 WannaCry exploit provides a compelling example of how Celerium's Predictive Analytics can identify a malicious IP before it's highlighted as problematic on traditional threat intelligence lists."

COMMUNITY ANALYTICS

One of the most unique capabilities of Network Defender comes in the approach we call "Community Analytics." In August of 2020, we were granted a patent for our unique approach to anonymizing our customers' data in a real-time data set. With a real-time data set of anonymous customer data, we can do some very interesting things to improve the accuracy of our scoring and to remove false positives from the data set. Further, because we categorize our customers into size (small, medium, and large) and sector (financial services, healthcare, IT, as examples), we are able to identify and research abnormal behavior in the community.

With respect to false positives, we have created a noise filter using our community data. This noise filter allows us to compare scoring we get from Signals-Based Threat Intelligence and Predictive Analytics against real- time network traffic. For example, if, for some bizarre reason, Google's primary IP for DNS 8.8.8.8 appeared on a number of threat intelligence sources, automated methods would block that IP and break stuff for many, many people. CDN uses our community analytics to make the determination that this IP is way too noisy to be considered blockable with any confidence, and would ignore these reports.

"In August of 2020, we were granted a patent for our unique approach to anonymizing our customers' data in a real-time data set."

Visit www.celerium.com to learn more about how

Celerium's Cyber Defense Network™ can help your organization be proactive in the fight against cyber threats.

CELERIUM.com