WHITE PAPER

Black Lotus Labs® Threat Intelligence: Risk Scores

John Spencer - Director of Product Management, Security

LUMEN®

Table of contents

Executive summary

Black Lotus Labs, the threat research arm of Lumen, generates threat intelligence to help protect businesses and keep the internet clean. This threat intel is integrated into many of the cybersecurity products sold by Lumen, such as Lumen Defender ℠ and Lumen® DDoS Mitigation Service. Black Lotus Labs processes data flows from the vast Lumen network and applies advanced machine learning algorithms to detect internet-based hosts and infrastructure being used by malicious actors. These hosts are then assigned a Risk Score that quantifies their severity. This white paper discusses the various parameters that affect these Risk Scores and the dynamic adjustments that are made throughout the threat event lifecycle.

Terms used in this paper

Adversary: A person or organization that perpetrates cyber threats for their own gain. The penalty for their actions should be a prison sentence or a hefty fine.
Asset: A technical computing or communication device – server, laptop, tablet, smartphone or other device that is automated and has the ability to communicate.
Command and control (C2) server: A server used by an adversary to control botnets and other infected target assets.
Indication of compromise (IoC): Reputation data for a specific public IP address, domain or sub-domain that indicates the entity is involved in potentially malicious activity or is a confirmed threat.
Kill chain: The progression of activities an adversary perpetrates to infect target assets for their gain.
Reputation data: Any information associated with an entity (IP, domain) on the public Internet. This data can be threat-based, positive, or neutral and is used to compute the overall Risk Score of an entity.
Target: An asset or organization that is the subject of a cyber threat.

How is a risk determined?

Broadly speaking, the Lumen Defender Risk Score is a combination of three major factors: severity, confidence and time.

Severity

Several subfactors combine to produce the severity factor of the risk score, including:

Threat category

- Primarily determined by how far the adversary has progressed down the Kill Chain. For instance, a "Scan" threat category is not (yet) very dangerous as the adversary is early in the attempt to penetrate the target's peripheral defenses.
- On the other end of the scale, a high volume (by byte count) conversation between a target asset and an adversarial command and control (C2) server may indicate data exfiltration – a very serious situation that has progressed far down the Kill Chain.
- The progression of threat categories includes Proxy, Scan, Phish, Malware, Bot, Attack and Command and Control (C2).

Positive rating

- You must take into consideration the network architecture that the address is in support of when reporting reputation at an IP Address level.
- If the IP Address is associated with a single server, then there is a high correlation between the threat event and the IP Address.
- But if the IP Address is associated with a hosting or CDN service, there may be large quantities of servers hosted behind that IP Address, lessening the likelihood that the target asset is interacting with the malicious device that is the subject of the threat event.

Confidence

Several subfactors combine to develop the confidence factor of the Risk Score.

Source confidence

- The Black Lotus Labs Threat Research Team assesses each source before including it in the reputation data. Each source is assigned a confidence factor based on its reputation and past abilities to correctly predict and determine malicious activities. Sources that are validated and determined to be highly accurate are given a high confidence factor. The higher the confidence we have in the source, the higher the contribution that source provides to the overall Risk Score.

Validation

- When a new malicious entity is reported, the Black Lotus Labs Threat Research Team attempts to validate the new entity and discover more about it.

- Typically, a surrogate asset is spun off in a sandbox which is used to reverse engineer the dialog to the suspected malicious entity.
- If the entity responds, then the confidence factor of the risk score is elevated.

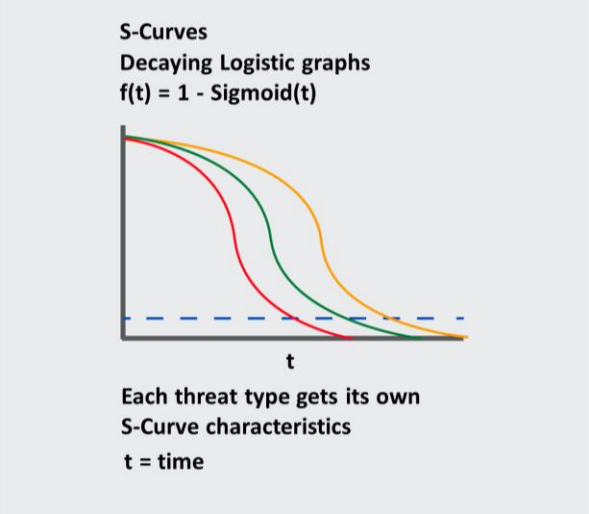
Risk score decay over time

It is imperative that threats be removed from the threat set in a timely manner. Internet-based threats are typically transient, and threat actors will frequently relocate their hosts to avoid detection. An IP address that is malicious today might be safe next week. As IP addresses cease to exhibit risky behavior, their risk scores should decrease over time.

Our research shows that the duration in which a threat is relevant varies between threat categories, indicating that the best practice is to commence the decaying process when the difference between the last notification of the threat and the current time exceeds a pre-defined interval that is unique to the category. The threat continues to decay over an S-Curve. Each Threat Category has its own S-Curve characteristics as depicted in the graph below.

S-Curves

See the S-curve characteristics for each threat category.



S-Curve characteristics include the steepness of the curve and the total height of the curve. Decaying S-Curves are known as “inverse logistics” curves in mathematics, which are driven by “inverse Sigmoid” functions (a little “geek candy” for readers who are so inclined). Once the Risk Score decays below a predefined threshold, it is removed from the Threat Set.

Conclusion

While there is a significant amount of leading-edge research and development that goes into the determination of accurate and relevant Risk Scores, the result for Lumen customers is the availability of a simple, actionable metric for quantifying the danger associated with an internet-based host. Risk Scores from Black Lotus Labs enable customers to see potential threats before they become breaches, because we are continuously sourcing information from one of the largest IP backbones in the world. The validation and original threat discovery done by the Black Lotus Labs team drives the fidelity of this information to an industry leading level.

Why Lumen?

In today's digital landscape, where threats evolve rapidly, Lumen Defender stands out as a beacon of proactive protection. Powered by the unmatched network visibility of Black Lotus Labs, Lumen Defender is not just a service – it's a strategic defense mechanism tailored to safeguard your business against the unknown.

866-352-0291 I lumen.com I info@lumen.com

LUMEN®