2020 STUDY SIXGILL

2020 STUDY

HOW DARKFEED'S UNIQUE INDICATORS ACCELERATE PROTECTION FROM THREATS

By Sumukh Tendulkar, Dov Lerner

Threat Intelligence has become a core element of any modern-day SOC.

SOC practitioners use threat intelligence feeds to proactively block known threats from their environment and to detect presence of malicious indicators in their network. Nowadays, these feeds are integrated with SOARs, SIEMs, TIPs, and other elements of security infrastructure, reducing barriers and increasing their adoption. Not surprisingly, many SOCs have multiple threat intelligence feeds. In fact, some SOCs consume as many as 40 or more.

Uniqueness

However, quantity of feeds does not necessarily promise quality of protection. There is substantial overlap between most feeds on the market. Consuming redundant feeds wastes valuable resources including time and money. Therefore, when seeking to add a new intelligence feed to your organization's portfolio, it is essential to understand how it differs from your existing solutions. Does it gather its data from a unique source at a different time in the kill chain? Does it provide unique indicators of compromise?

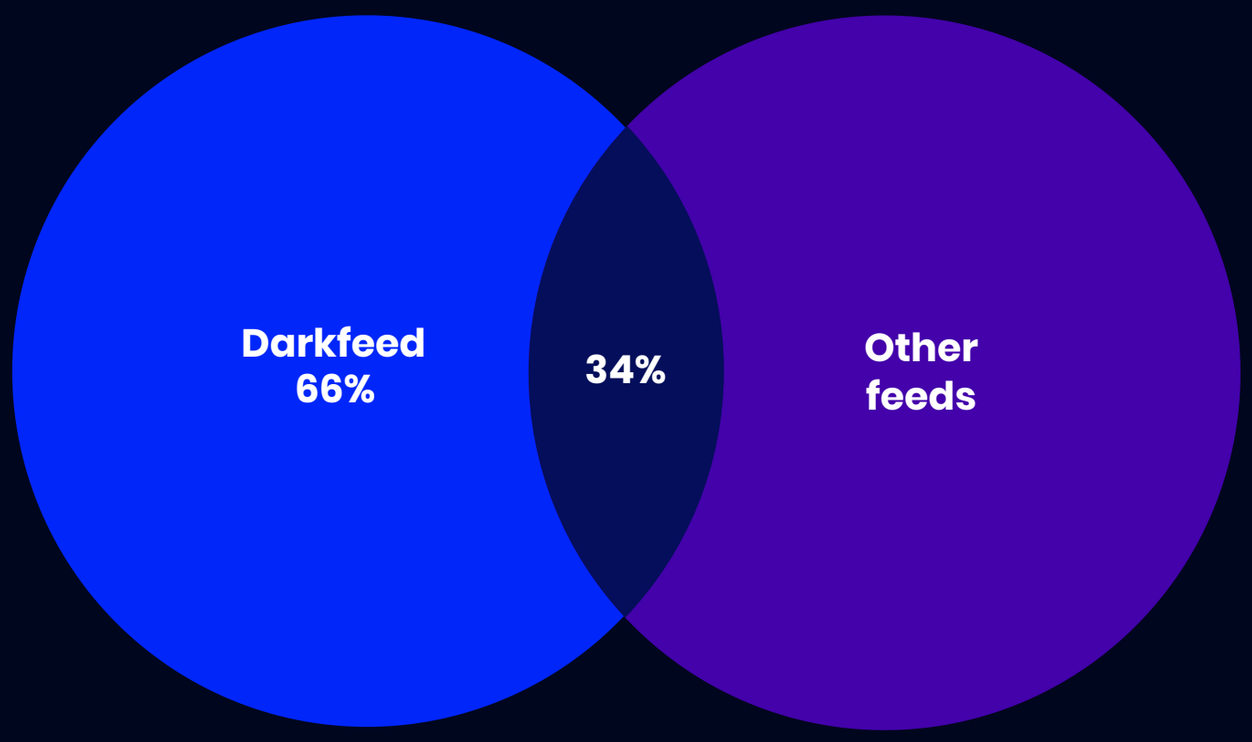
To these questions, Darkfeed answers an emphatic "Yes!"

The Darkfeed Solution

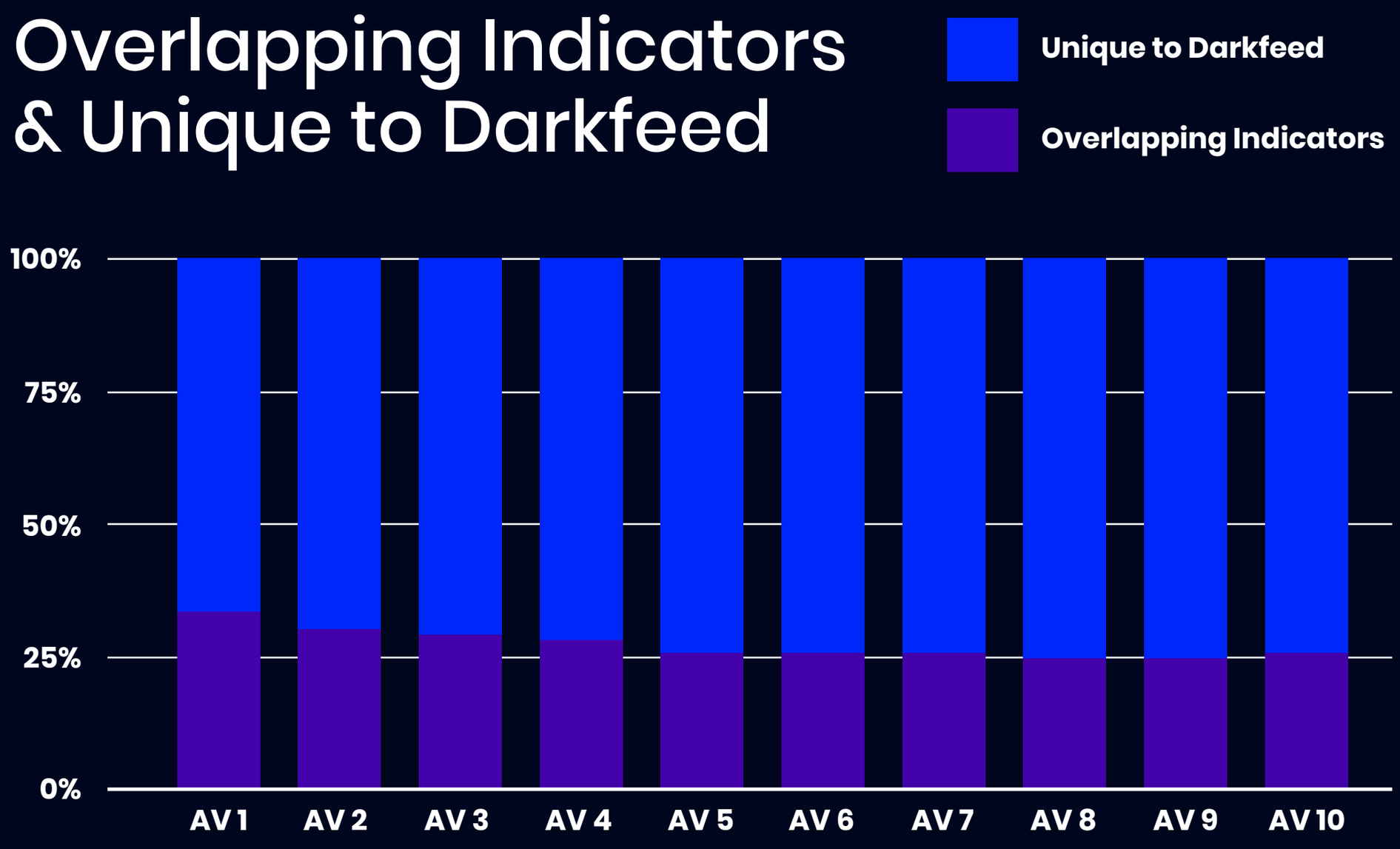
Most TI feeds are generated from telemetry—a network of sensors, such as endpoints or honeypots, that detects attacks in progress. Darkfeed, however, is sourced from chatter among cybercriminals in underground sources (commonly referred to as deep and dark web markets, forums, and messaging platforms). Darkfeed's visibility into this unique data realm captures the indicators at a much earlier stage in the kill chain. This includes domain names or access to compromised domains and RDP connections, which are distributed on underground forums for other actors to acquire and weaponize with a phishing page, C2 server, or malware hosting. Furthermore, Darkfeed includes hashes of malware captured when an actor discusses it or boasts about its undetectability in an underground forum. By focusing on the early stages of the malicious supply chain, many of Darkfeed's indicators are not only unique, but proactive—alerting to an IOC days or even months before it is used in an attack and detected by traditional telemetry.

Results

The highest instance of overlap we found with any single anti-virus was an overlap of 34%. In other words, a full ⅔ of Darkfeed was unique (fig 1). The overlap with other sources of indicators was even lower as illustrated in fig 2.



This is a remarkable rate of unique IOCs, considering that this is a comparison to one of the most widely used anti-virus engines. Further, the uniqueness increases in head-to-head comparisons with individual security vendors; only ten individual vendors reported over 25% of these IOCs as malicious:



2020 STUDY SIXGILL

Darkfeed - The Last Feed You Will Ever Need

• Automatically integrate IOCs into your security stack (machine-to-machine)
• Improve your SOAR, SIEM & Vulnerability Management System with seamless integration of Sixgill's contextual data
• Receive automated early warnings of new malware threats
• Get actionable insights to effectively mitigate threats
• Level-up your threat hunting for malicious IOCs in corporate networks
• Better understand malware TTPs and trends
• Expandable and future-proof with continuous additions and intel stream enrichment

Uniqueness of a threat intelligence stream is crucial to ensure proper coverage against the widest spectrum of threats, and to eliminate wasted hours. Darkfeed's distinct source of information from underground activities and its automated machine-machine approach with proven uniqueness makes it an important part of SOC infrastructures. Indeed, it is the last feed you will ever need.

About Sixgill

Sixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response — in real-time. Sixgill's investigative portal empowers security teams with contextual and actionable alerts along with the ability to conduct real-time, covert investigations. Rich intelligence streams such as Darkfeed™ harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

Sixgill Darkfeed is the industry's most comprehensive deep and dark web threat intelligence stream. With Darkfeed, SOC professionals can get real-time, actionable insights to block items that threaten their organization. Darkfeed harnesses Sixgill's unmatched intelligence collection capabilities both in terms of breadth and quality. Its contextual threat intelligence is highly accurate, comprehensive, covert and automated. The feed is structured in the STIX format allowing users to automatically consume and integrate it with their security systems, processes and methodologies.

Want to learn more?

REQUEST A DEMO