SIXGILL

Darkfeed

by Sixgill

Product Data Sheet

SIXGILL

Darkfeed by Sixgill:

DETECT AND OBLITERATE THREATS AND MALICIOUS IOCs

Automated | Actionable | Comprehensive | Real-time

Darkfeed is a feed of indicators of compromise (IOCs), including malicious domains, URLs, IP addresses, and file hashes.

These IOCs are automatically extracted from Sixgill's deep, dark and surface web sources. Darkfeed is automated, meaning that IOCs are extracted and delivered in real-time, and it is actionable, in that you will be able to receive and block items that threaten your organization.

Darkfeed harnesses Sixgill's unmatched intelligence collection capabilities both in terms of breadth and quality. Darkfeed's contextual threat intelligence is highly accurate, comprehensive, covert and automated.

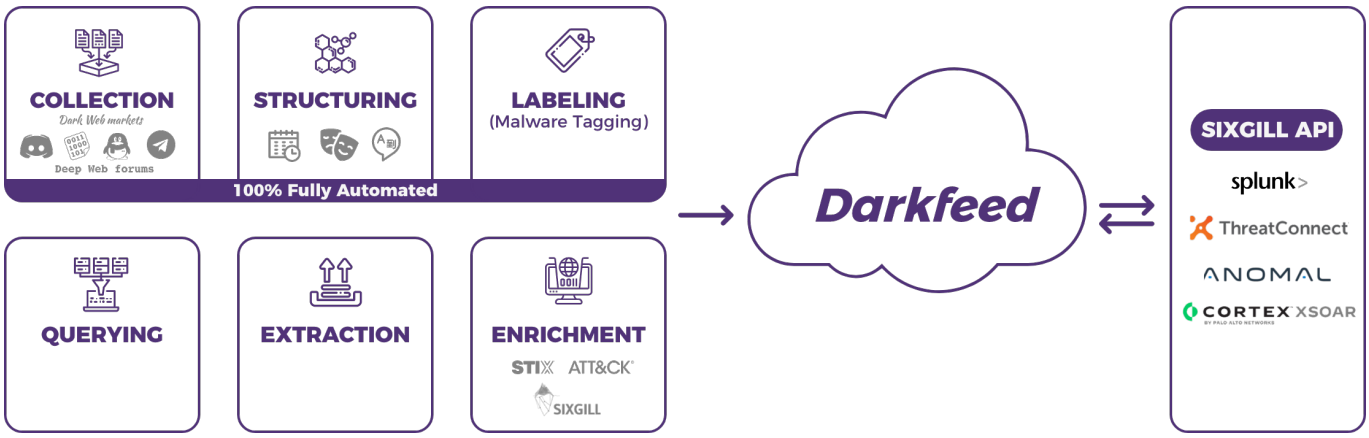
The feed is structured in the STIX format and shared via Sixgill's API, allowing customers to automatically consume and integrate it with their security solutions, whether SIEM, SOAR, vulnerability management tool, or any other platform.

BENEFITS

- **Automatically integrate IOCs** into your security stack (machine-to-machine)
- **Improve your SOAR, SIEM and Vulnerability Management efficiency** 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 feed enrichment

SIXGILL

ARCHITECTURE & INTEGRATIONS



Darkfeed can seamlessly integrate with all major TIP, SIEM and SOAR platforms. Missing one of your systems here? Ask about our quick and custom integration program.

Darkfeed is automated and transparent. It seamlessly integrates into your existing enterprise security stack and fits into the normal flow of your SOC without change or interruption. The feed is structured in the STIX format for automated parsing, custom properties (feed name, feed ID, post title, actor, source, etc.) for IOC enrichment and filtering, as well as external integrations for IOC enrichment (Mitre ATT&CK, Virustotal, & more).

FEED CONTENT

Domains

- Compromised sites to which access is sold on the dark web
- Suspicious domains that are for sale on the dark web

URLs

- Links to malware files hosted on underground file-sharing sites

Hashes

- Malware hashes
- Hashes of malware claimed to be undetected

IP addresses

- Command-and-control server IP addresses for most prevalent malware
- Command-and-control server IP addresses for servers involved in botnets, DDoS attacks, and proxy anonymization

SIXGILL

VISIBILITY INTO YOUR THREATSCAPE

Gain total visibility of the threatscape of your organization, industry and more. Mitigate threats in advance, prevent incidents and minimize attack surface.

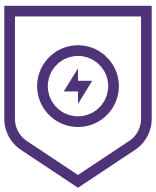
FUEL YOUR ANALYTICS

Use the data to track, trend and gain data-driven actionable insights to the IOCs collected by Darkfeed. Gain better understanding of malware TTPs and trends.

SECURITY

We treat the security of data with the highest standards. Sixgill's security-first approach leverages the best and most advanced technologies to make sure that your data stays safe and private. Our service undergoes rigorous audits and employs the latest best practices to ensure the integrity of the data as well as its authenticity, security and compliance.

Confidential



Secured

Information Security management system

Sixgill is a fully automated cyber threat intelligence solution suite that helps organizations protect their critical assets, reduce fraud and data breaches, protect their brand and ultimately minimize attack surface. The platform empowers security teams with contextual and actionable insights as well as the ability to conduct real-time investigations. Rich data feeds such as Darkfeed™ harness Sigill's unmatched intelligence collection capabilities and delivers real-time intel into organizations' existing security systems to help proactively block threats. Current customers include global 2000 enterprises, financial services, MSSPs, governments and law enforcement entities.