DuskRise

Disrupt the Adversaries Before They Disrupt You

Cluster25 counter threat intelligence enables organizations to make fast & informed decisions to protect their assets and stakeholders.

Powered by Cluster25

On the lookout for threats, 24/7.

Cluster25 Advanced Threat Research team continually probes the Clear, Deep and Dark web to capture new indicators of compromise, emerging threats, relevant adversaries, evolving tactics and targeted campaigns. The gathered insights provide real-time alerts, proactive response, and tailored reports that help secure the infrastructure and assets of our customers, from IGOs to SMBs.

Actionable intelligence at your fingertips

DuskRise's curated counter threat intelligence, powered by both SIGINT and HUMINT, integrates seamlessly with downstream security controls to actively block ransomware, phishing and other malicious attacks.
Our cutting-edge platform helps reduce downtime, data loss, reputational damage, false positives, MttD and MttR.

Complete, relevant and accessible coverage tailored to your business

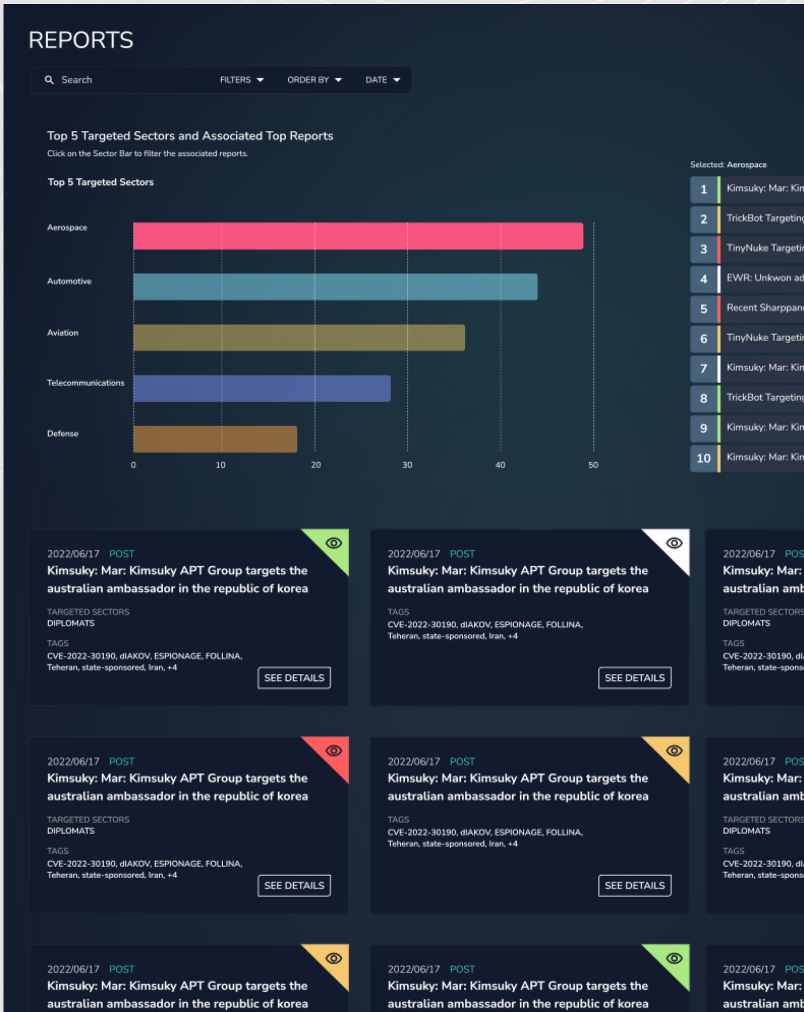
- » Dark & Deep web actionable intelligence
- » Triage tools for SOC analysts
- » Scalable AI / ML to reduce risk for your organization
- » Customized detection rules for varied technology stacks
- » Actionable malicious observables with a STIX / TAXII feed
- » Disruptive intelligence

Counter threat intelligence

Nation-state caliber automated cyber defense for Main Street

Today, when individuals have access to nation-state caliber malware, organizations of all scales need to employ the most advanced technology out there to protect themselves.

DuskRise operationalizes intelligence by processing massive data sets and detecting threats most relevant to your tech stack, industry, and brand.



Top 5 Targeted Sectors and Associated Top Reports

Click on the Sector Bar to filter the associated reports.

Top 5 Targeted Sectors

Selected: Aerospace

1	Kimsuky: Mar: Kin
2	TrickBot Targeting
3	TinyNuke Targetin
4	EWR: Unkwon ad
5	Recent Sharppan
6	TinyNuke Targetin
7	Kimsuky: Mar: Kin
8	TrickBot Targeting
9	Kimsuky: Mar: Kin
10	Kimsuky: Mar: Kin

2022/06/17 POST
Kimsuky: Mar: Kimsuky APT Group targets the australian ambassador in the republic of korea
TARGETED SECTORS
DIPLOMATS
TAGS
CVE-2022-30190, dIAKOV, ESPIONAGE, FOLLINA, Teheran, state-sponsored, Iran, +4

2022/06/17 POST
Kimsuky: Mar: Kimsuky APT Group targets the australian ambassador in the republic of korea
TAGS
CVE-2022-30190, dIAKOV, ESPIONAGE, FOLLINA, Teheran, state-sponsored, Iran, +4

2022/06/17 POS
Kimsuky: Mar:
australian amb
TARGETED SECTORS
DIPLOMATS
TAGS
CVE-2022-30190, dI
Teheran, state-spons

2022/06/17 POST
Kimsuky: Mar: Kimsuky APT Group targets the australian ambassador in the republic of korea
TARGETED SECTORS
DIPLOMATS
TAGS
CVE-2022-30190, dIAKOV, ESPIONAGE, FOLLINA, Teheran, state-sponsored, Iran, +4

2022/06/17 POST
Kimsuky: Mar: Kimsuky APT Group targets the australian ambassador in the republic of korea
TAGS
CVE-2022-30190, dIAKOV, ESPIONAGE, FOLLINA, Teheran, state-sponsored, Iran, +4

2022/06/17 POS
Kimsuky: Mar:
australian amb
TARGETED SECTORS
DIPLOMATS
TAGS
CVE-2022-30190, dI
Teheran, state-spons

2022/06/17 POST
Kimsuky: Mar: Kimsuky APT Group targets the australian ambassador in the republic of korea

2022/06/17 POST
Kimsuky: Mar: Kimsuky APT Group targets the australian ambassador in the republic of korea

2022/06/17 POS
Kimsuky: Mar:
australian amb

Brand intelligence

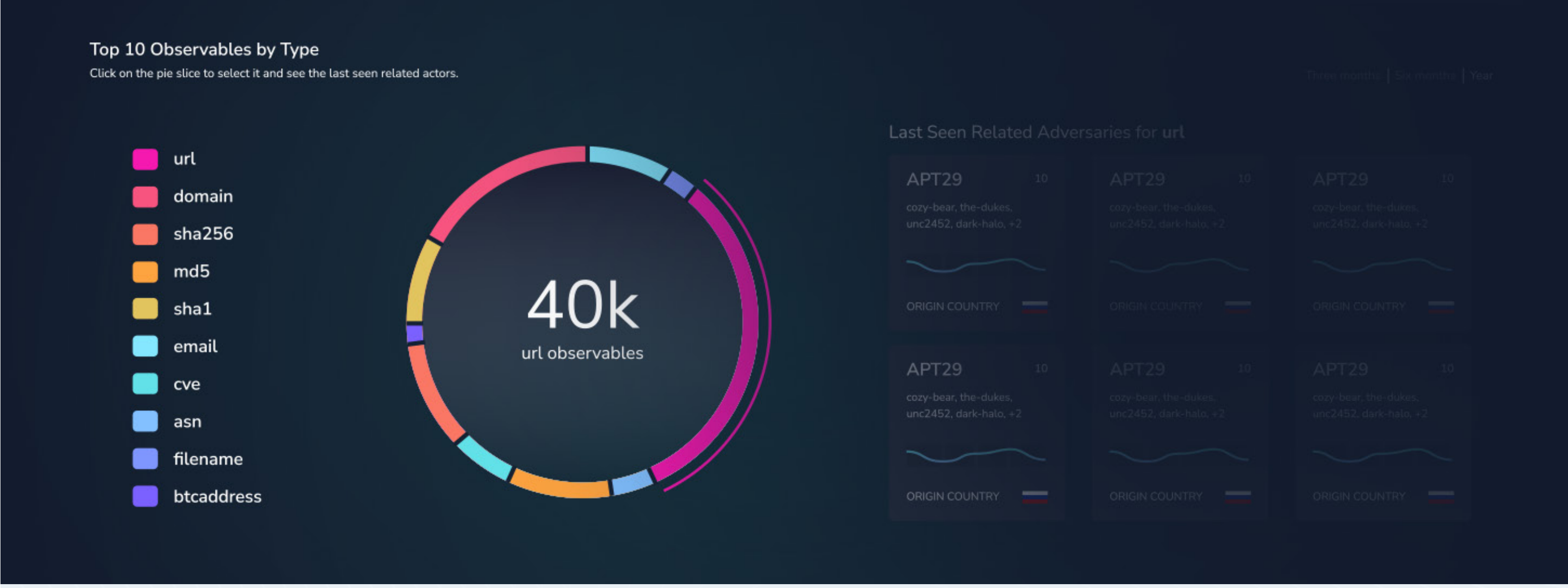
Protect your good name

We combine AI algorithms and human expertise to collect and analyze data points across a wide range of sources, including the Surface, Deep and Dark web, mobile application stores, and social media, in order to identify potential risks for your brand, people, and intellectual property.

Unique features

- Typosquat Domain Monitoring - Continuous monitoring and alerting for lookalike domains, counterfeit websites, and cert registration.
- VIP Monitoring - Protect executives and other VIP stakeholders from targeted cyber and other threats, including online impersonation.
- Rogue Apps Monitoring - Continuous monitoring of App Store, Google Play Store, and gray APK sites for fake and / or malicious apps.
- Social Media Monitoring - Continuous brand and VIP monitoring and alerting for social media impersonation.
- Leaked Credentials Detection - Continuous monitoring and alerting for relevant leaked credentials in dumps and for sale in dark web markets.
- Doxing - Thwart hacktivists and disgruntled employees with continuous monitoring for sensitive data leaks.
- Leaked Code Detection - Continuous monitoring and alerting for accidental or intentionally leaked code.
- Managed Takedown Service - Takedown domains, fake social media profiles, and rogue apps.

2 LokiBot
3 Dridex
4 FORMBOOK
5 Qakbot
MAG
GIU
LUG
AGO
SET
OTT
NOV
Three months / Six months / Year
See all
Sectors & Associated Malwares
bazarloader: X events
RMBOOK
5 Qakbot
SET
OTT
NOV
Three months / Six months / Year
See all
3
4 EWR:
5 Recent Shar
6 TinyNuke Targeting
7 Kimsuky: Mar: Kimsuky A
8 TrickBot Targeting Update Septe
9 TinyNuke Targeting Update September
10 Kimsuky: Mar: Kimsuky APT Group targets the
See al
Three months / Six mo



Top 10 Observables by Type

Click on the pie slice to select it and see the last seen related actors.

Three months | Six months | Year
url
domain
sha256
md5
sha1
email
cve
asn
filename
btcaddress
40k
url observables
Last Seen Related Adversaries for url
APT29 10
cozy-bear, the-dukes, unc2452, dark-halo, +2
ORIGIN COUNTRY
APT29 10
cozy-bear, the-dukes, unc2452, dark-halo, +2
ORIGIN COUNTRY
APT29 10
cozy-bear, the-dukes, unc2452, dark-halo, +2
ORIGIN COUNTRY
APT29 10
cozy-bear, the-dukes, unc2452, dark-halo, +2
ORIGIN COUNTRY
APT29 10
cozy-bear, the-dukes, unc2452, dark-halo, +2
ORIGIN COUNTRY
APT29 10
cozy-bear, the-dukes, unc2452, dark-halo, +2
ORIGIN COUNTRY

Fraud intelligence

Limit or prevent financial loss

Compromised credit cards, bank accounts, and other sensitive data and assets present a high risk to the integrity of an organization, regardless of its size and scale of operations. By harnessing the power of the DuskRise counter threat intelligence you can remain one step ahead of cybercriminals and mitigate possible losses and liabilities.

Unique features

» Compromised Credit Card Detection - Detect when credit cards have been compromised as part of a data dump or are for sale on the Dark web.

» Fraud Detection via Historical Analysis - Knowing the timeline of when a credit card was first compromised helps identify suspected fraudulent transactions.

» Pre-CAMS Alerts - Our Fraud Intelligence often detects compromised cards before Compromised Account Management System (CAMS) alerts are sent to banks or merchants.

» Compromised Bank Account Detection - Know whether your customer's login credentials and / or account email have been compromised on the Dark web.

» Rogue App Detection - Detect rogue apps in App Store, Google Play Store, and gray market APK websites.

» Fraudulent Website Detection and Takedown - Quickly detect and remove fraudulent websites and apps.

» Automated FMS and PoS Enrichment - API queries provide real-time contextual enrichment of the Fraud Management System (FMS) and Point-of-Sale (PoS).

DuskRise

DuskRise covers a new gap in enterprise security that has been exposed by the shift to work from home. Building on the expansion of the enterprise from traditional endpoints, to IoT and BYOD, DuskRise empowers Security and Operations teams to make sure these remote networks, and any device on them, are secure.

Powered by its own Cluster25 threat research and intelligence, companies can extend security to the edge of the network, with a seamless integration process and a beautiful user experience.

DuskRise is enabling a secure workforce without boundaries.
Learn more at DuskRise.com.

Get a demo
https://get.duskrise.com

Product inquiries
sales@duskrise.com

Contact information
331 Park Avenue South, Floor 4,
New York, 10010