whoami

user=dnicholson role=Solutions Engineer org=Abnormal AI

David Nicholson

Solutions Engineer

BACKGROUND

20-something years running IT and Security in Defense & Healthcare Manufacturing.

(So much SCADA)

VENDOR SIDE

13+ years

9 years @ RSA NetWitness Platform — full packet capture, SIEM, and EDR.
4.5 years @ Abnormal AI — Behavioral AI SOC automation.

COMMUNITY

10-year DEF CON attendee

3-year RSAC SOC & Black Hat NOC analyst.

Show deskto

whoarewe

uid=abnormal.ai founded=2018 mission="use good AI to stop bad AI"

Behavioral AI, built for cyber defense

Founded in 2018 by AI insiders — the belief that AI that understands normal human behavior is the strongest defense against the attacks that exploit it.

FOUNDED

2018

AI-native from inception, by behavioral AI experts.

SCALE

5,000+

Enterprise organizations protected, including more than 25% of the Fortune 500.

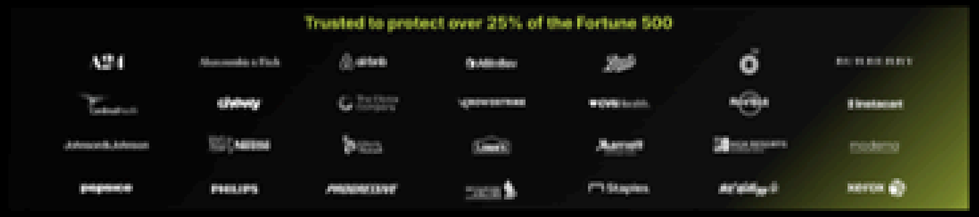
RECOGNITION

Gartner

Leader in the Magic Quadrant for Email Security Platforms; 99% Would Recommend on Gartner Peer Insights.

[The Leader in Email Security]





The Abnormal Behavioral Security Platform

Behavioral AI that protects email, identity, and AI — and stops insider threats.

Threat Intelligence | AI Supervisors | Detection Tuning | Threat Hunting | Threat Research

Email Security

Stop BEC, phishing, and account takeover attacks.

Identity Security

Harden identities, detect compromise, and prevent threats.

AI Security

See every AI tool and enforce policy.

Insider Threat

Block fraudulent actors and malicious insiders.

Abnormal Behavior Platform
Powered by **Attune 1.0**

Behavioral Detection & Response	AUTONOMOUSLY ADDRESSES ANOMALIES IN REAL-TIME
Behavioral Modeling	BUILDS BESPOKE BASELINES TO DEFINE "NORMAL"

Cloud-Native API Architecture

INGESTS THOUSANDS OF BEHAVIORAL SIGNALS IN ONE CLICK

Microsoft · Google · Okta · Slack · AWS · Zoom · Salesforce · Splunk · Box · Workday · ServiceNow

THREAT INTELLIGENCE

Platform Unifier

Enabling Feedback Loops



Every threat uncovered makes detections smarter. Every detection improves protection. Every signal strengthens the next hunt. **The loop never stops.**

[TURNING SIGNALS INTO STORIES]

Unlocking the full value of threat intelligence

Three engines turn telemetry into a structured, queryable model of the adversary.

[01]

Internal & External Collection

Model the behavior of tools, techniques, and threat actors by collecting signals across sources.

- Extract attacker infra, tools, TTPs from internal datasets
- Enable OSINT, active attacker engagement, partner feeds

[02]

Diamond Modelling

Structure threats so analysts can pivot across the four edges of the diamond.



Correlate internal & external data to drive detection, hunting, and response.

[03]

Intel DB

Store enriched intel and campaigns with long-term context.

- Retain attack data long term
- Enable pivoting, clustering, campaign recall
- Power intelligence-enabled products

Product | Every piece of intelligence — internal or external — ships as a product.

Abnormal

The Return of Kratos

Abnormal Threat Intelligence



- Microsoft 365 AiTM phishing-as-a-service
- Sneaky2FA lineage · the franchise model

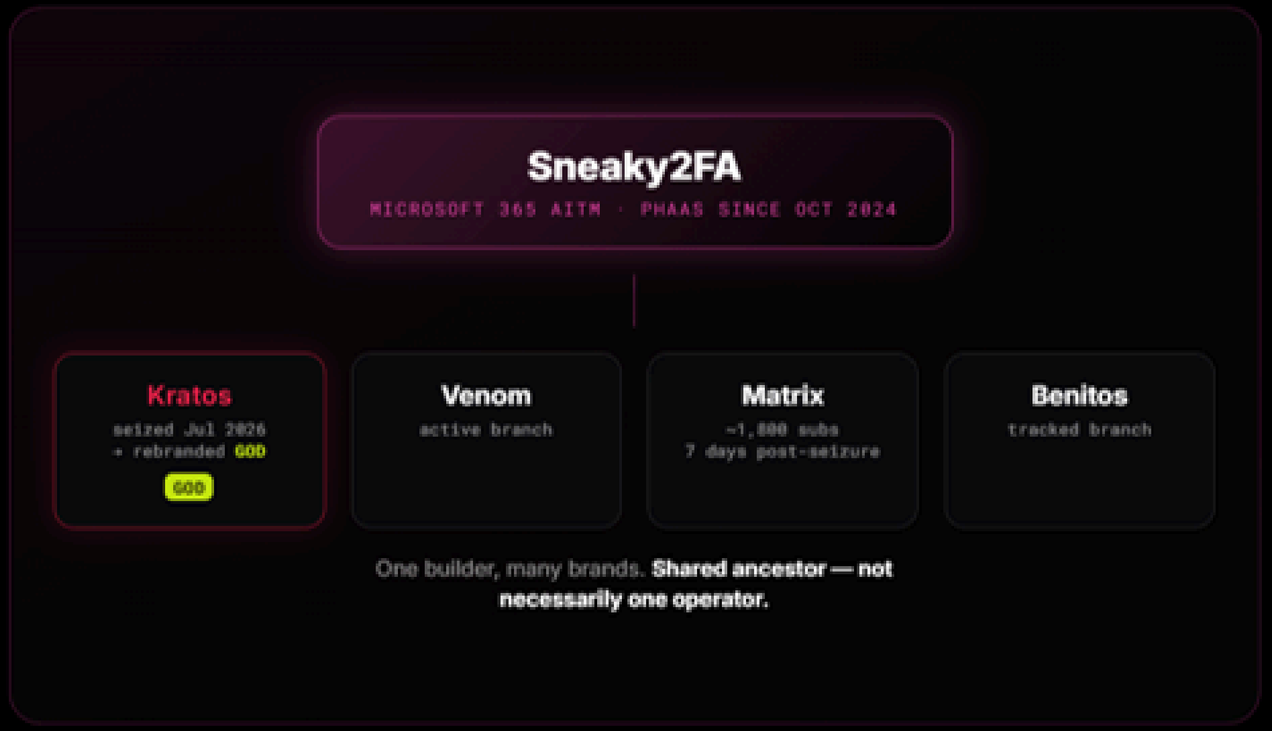
THREAT INTELLIGENCE · CASE STUDY

The Return of Kratos

A Sneaky2FA-lineage phishing franchise — incredibly popular by February, seized by international law enforcement in July, back in September under a new name.

Phishing, sold as a franchise

Kratos is not a lone kit. It is one rented brand of the **Sneaky2FA** lineage — a phishing-as-a-service codebase that affiliates re-skin and host themselves. That structure is exactly why taking down one platform doesn't end the threat.



A reseller economy

- Affiliates ("agents") license the kit and resell it on commission — onboarded and supported over **Telegram**, paid in **cryptocurrency**.
- A few clicks deploy a fake Microsoft 365 login: pick an anti-bot gate, set geo-filters, install SSL, route stolen data to a Telegram bot.
- **Decentralised by design.** Take down one affiliate and the rest stay up — like franchise stores after head office burns down.

How we read the family

- Every Sneaky2FA-lineage panel ships a `k.png` at `/admin/assets/images/`. The image tells us **which branch and which affiliate**.
- The operator login's **"register code"** is base64 of the server's own IP — it leaks the origin host hiding behind Cloudflare.

PROPRIETARY · BUSINESS SENSITIVE · DO NOT DISCLOSE

By February, it was everywhere

Kratos emerged as the Sneaky2FA successor and scaled like a product — rented by roughly **1,800 affiliates** running an estimated **15,000 campaigns a month**.

A representative February campaign

- **~100 organizations**, mostly in the U.S. — manufacturing, retail and healthcare.
- Tax-season lure: each email carried a **W-2 document with a QR code personalised to the recipient**.
- The QR led to a fake Microsoft 365 sign-in — an **AiTM** page that relays the login live and steals the session **after** MFA.

Why it worked: AI-generated lures, per-recipient personalisation, and real-time MFA bypass — shipped as a turnkey subscription.

Rented like SaaS

- Dashboard deployment, SMTP rotation, anti-bot and geo-filtering, token vault with session refresh.
- Subscription pricing in the **low hundreds per month**, billed in crypto, supported over Telegram.
- Victims confirmed across **30+ countries** — mostly Europe and the U.S.

~1,800
AFFILIATE SUBSCRIBERS
Each brands & hosts its own instance

~15,000
CAMPAIGNS / MONTH
Across the lineage at peak

30+
COUNTRIES HIT
Mostly Europe & the U.S.

€300K+
SUBSCRIPTION FEES
Collected since 2024

Seized by international law enforcement in July.



The seizure notice placed on the platform's own domain — **FBI**, **U.S. DOJ**, Germany's **BKA** and the Frankfurt **ZIT**. Note the artwork the investigators chose: **Kratos face-down beneath the blade.**

JUL 2026	**Operation Olympus Blade.** Frankfurt's ZIT and Germany's BKA, with the FBI — and the lead developer arrested in Indonesia.
INFRASTRUCTURE	**200+ servers** seized; the central infrastructure and primary domain taken under warrant.
SCALE	At takedown: **~1,800 subscribers**, **~15,000 campaigns/month**, victims in **30+ countries**; **€300K+** in subscription fees since 2024.
THE NAME	*"Olympus Blade" is the weapon Zeus uses to kill Kratos in* God of War. **The investigators made the first move — and the first reference.**

Decapitation, not death

Seizing the central infrastructure takes the builder's head — but the affiliates each run their own branded, self-hosted instances. The franchise outlives head office.

[KRATOS · SEPTEMBER 2026]

Attacking you in September — under a new name.

Same builder, same panel, a new skin. Two operator consoles answered on the same day — one still branded Kratos, the one attacking in the wild rebranded **GOD**.



Kratos

`admin/assets/images/k.png`
7,608 bytes · a sibling still carrying the seized brand



GOD

`admin/assets/images/k.png`
2,002 bytes · the console attacking in the wild

Identical directory layout, identical operator sign-in contract. **The image is the only thing that changed.** Byte-for-byte, these are the same build — first-party, captured by Abnormal.

The name is a joke at the investigators' expense

"Kratos" is the protagonist of the *God of War* games — and the story runs in three beats, all three of which have now happened here.

1. **He becomes the God of War**
   Kratos kills Ares and takes his throne. → **a platform is named Kratos.**
2. **Zeus runs him through with the Blade of Olympus**
   The weapon that kills Kratos. → **the takedown is Operation Olympus Blade.**
3. **He claws out of the underworld and tears down Olympus**
   Kratos returns for the gods. → **the console attacking you is branded GOD.**

And the franchise re-skins faster than it can be named: **Matrix**, *another Sneaky2FA-lineage panel, stood up* **~1,800 subscribers within a week** *of the takedown.*

[KRATOS · WHAT IT MEANS FOR DEFENDERS]

You can't block a franchise. You can detect the behavior.

Domains, brands and panels rotate on demand — a seized "Kratos" is an attacking "GOD" two months later. What persists is the technique, and that is what behavioral AI models.

Known-good, acting wrong

- A sign-in completed at the **real** Microsoft from an address that isn't the user's.
- Session cookies issued, then reused from a **different network** minutes later.
- **AiTM steals the session after MFA** — a password reset alone does not contain it.

What actually generalizes

- Behavioral baselines over rotating infrastructure — not blocklists of disposable domains.
- Lineage fingerprints we hunt: the **k.png** family/affiliate marker and the **register-code origin leak**.
- Delivery tells: links smuggled in **SVG** or **nested message/rfc822** attachments, not the body.

Attribution, honestly

- Lineage is a **shared ancestor**, assessed from shared files plus public reporting — not proof of one operator.
- **Kratos → GOD** is byte-confirmed, first-party: same build, one changed image.
- **Matrix ↔ Kratos** is five identical files and 37/82 verbatim lines — strong, with an honest gap.

Sources. Public reporting on Operation Olympus Blade: The Register, BleepingComputer, Trend Micro, teiss, cyberpress, The Hacker News (Jul 2026). Sneaky2FA-lineage assessment per Sekoia, PCRisk and Trend Micro. Scale, delivery and panel findings from Abnormal first-party captures, June–September 2026. No credentials were submitted to any attacker system; third-party organisations named as victims are not participants.

Kratos Portal Demo



“Don’t play with Super Glue”

– Dr. Spock