



MAYER | BROWN

DISRUPTION IN ACTION: INSIDE MICROSOFT'S DIGITAL CRIMES UNIT

October 7, 2026

TODAY'S SPEAKERS



ADAM HICKEY

MAYER BROWN
PARTNER



CARLTON GAMMONS

MICROSOFT
PRINCIPAL CORPORATE COUNSEL,
DIGITAL CRIMES UNIT
FORMER ASSISTANT U.S. ATTORNEY,
MIDDLE DISTRICT OF FLORIDA

AGENDA

1. Digital Crimes Unit Overview
2. Common Causes of Action
3. Case Studies
4. Key Takeaways

The background is a complex digital-themed abstract. It features glowing orange and yellow circuit traces on the left side, transitioning into a dark blue field with lighter blue circuit patterns. On the right, there are vertical columns of glowing blue binary code (0s and 1s). A thin white vertical line runs down the center of the image, passing through the text.

01

DIGITAL CRIMES UNIT OVERVIEW

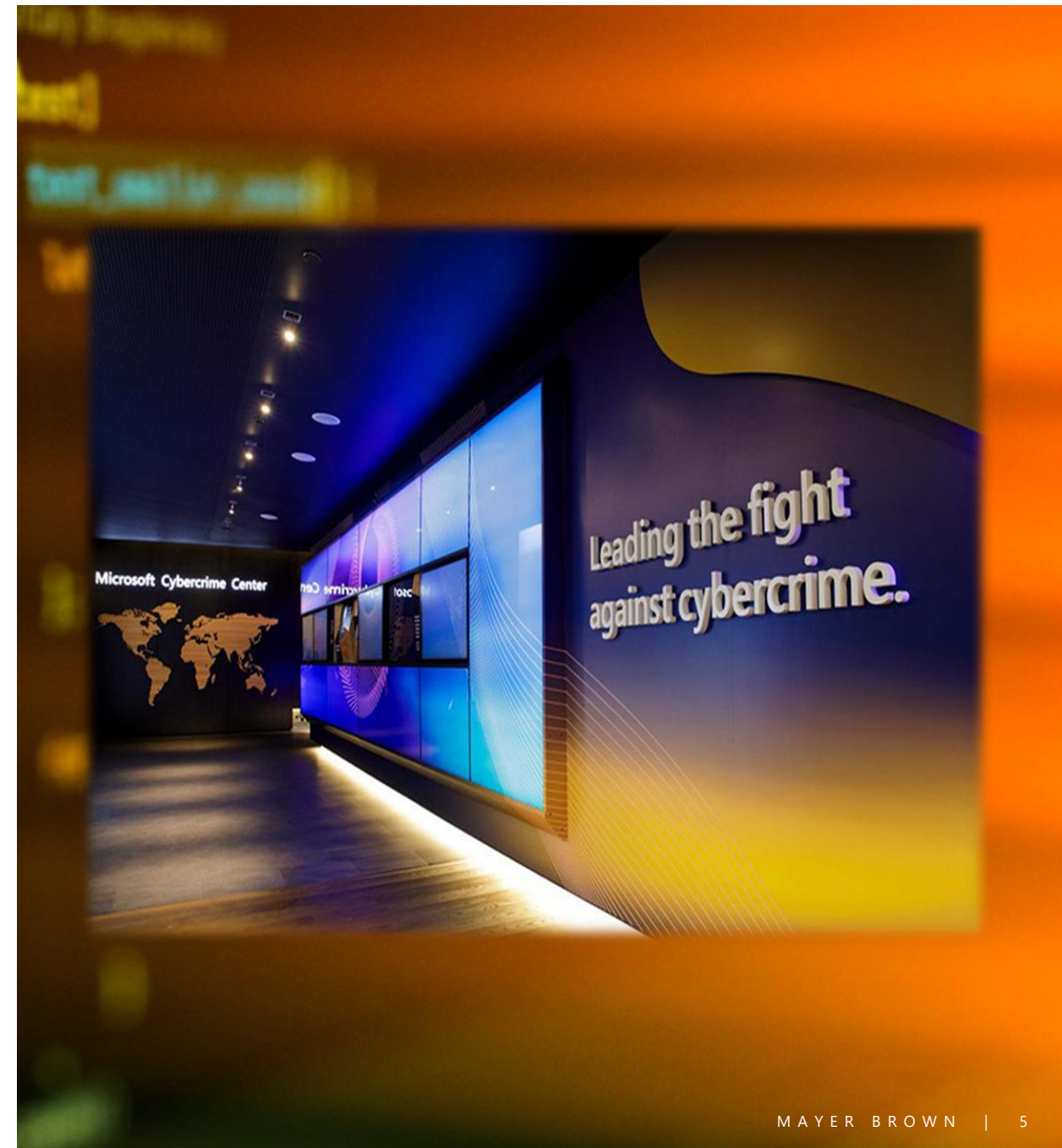
MICROSOFT DIGITAL CRIMES UNIT

- **Background**

- Comprises an international team of technical, legal, and business experts dedicated to combatting cybercrime.
- Leverages civil actions, technical interventions, criminal referrals, and public-private partnerships to protect Microsoft and its customers.
- Collaborates with the Microsoft Threat Intelligence Center (MSTIC) to identify and attribute threat actors.

- **Impact**

- 40 court-authorized disruptions.
- 30+ malware families and nation-state actors disrupted.
- 500M+ victim devices rescued.
- 780+ arrests in collaboration with law enforcement since 2014.



THE CIVIL DISRUPTION PLAYBOOK

01

File civil complaint under seal in federal district court.

02

Seek emergency ex parte TRO and order to show cause.

03

Obtain court authorization to seize/transfer domains and redirect traffic to Microsoft sinkhole.

04

Direct third-party infrastructure providers (registries, registrars, hosts) to act via court orders.

05

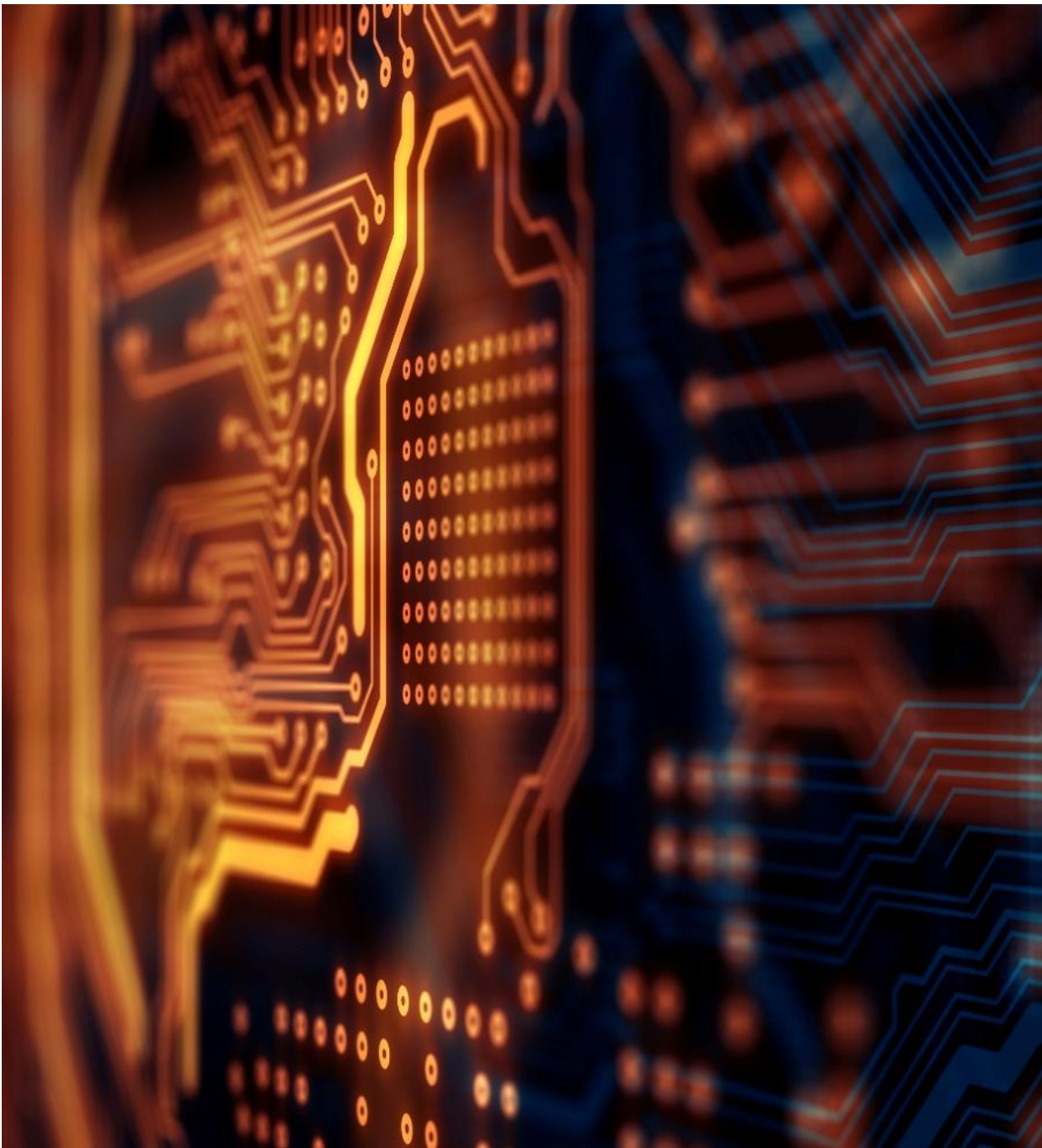
Unseal case and serve defendants.

06

Obtain preliminary injunction; seek appointment of court monitor to seize newly-created domains as actors reconstitute.

07

Obtain default judgment and permanent injunction.



WHY CIVIL LITIGATION?

Speed and Control

- Ex parte TRO can be obtained in days rather than months.
- Microsoft controls the litigation timeline, strategy, and scope.
- Civil causes of action give Microsoft standing to sue directly.

Parallel tracks

- Criminal referrals to law enforcement complement the civil disruption strategy.

Why ex parte and under seal?

- Notice would give defendants the opportunity to move infrastructure, destroy evidence, and render relief futile.
- Documented history of actors relocating targeted infrastructure once they learn of Microsoft's efforts.

The background is a complex digital-themed abstract. On the left, there are glowing orange and yellow circuit traces and patterns. On the right, there are blue and teal circuit traces and patterns. In the center-right, there are vertical columns of binary code (0s and 1s) in a light blue color. The overall color palette is dominated by warm oranges and yellows on the left, transitioning to cool blues and teals on the right.

02

COMMON CAUSES OF ACTION

RECURRING CAUSES OF ACTION

CLAIM	STATUTORY / LEGAL BASIS	ADVANTAGES
Racketeer Influenced and Corrupt Organizations (RICO)	18 U.S.C. § 1962(c)–(d) — predicate acts may include wire fraud and CFAA claims	Reaches the whole “enterprise”—developers, sellers and end-user purchasers of a malicious tool/service—in one complaint. Framing the operation as a coordinated scheme supports broad injunctive relief against every participant and the infrastructure they share.
Lanham Act	§§ 1114, 1125(a), 1125(c) — infringement, false designation, dilution	Misuse of Microsoft marks deceives customers, making the harm concrete and immediate (also allowing for emergency injunctive relief).
Computer Fraud & Abuse Act (CFAA)	18 U.S.C. § 1030	Reaches the unauthorized access itself and allows for injunctive relief.
Common Law Claims	Trespass to chattels; conversion; unjust enrichment; tortious interference; breach of contract (e.g., Microsoft Terms of Use)	Captures interference with Microsoft’s property and defendants’ profits. Fills gaps the statutes might have, supports disgorgement of ill-gotten gains, and ties defendants’ conduct to the Terms of Use.

The background is a complex digital-themed abstract. It features glowing orange and yellow circuit traces on the left side, transitioning into a dark blue field with faint, glowing blue circuit patterns. On the right side, there are vertical columns of glowing blue binary code (0s and 1s). A thin white vertical line runs down the center of the image, passing through the text.

03

CASE STUDIES

EVILTOKENS: AI-ENABLED PHISHING-AS-A-SERVICE PLATFORM

Microsoft Corp. & Health-ISAC v. Utomi, Adams & Does 1–5 | E.D. Va. | Filed in September 2026 | Storm-2992

THE SCHEME

- AI-enabled phishing-as-a-service sold on Telegram (\$1,500 initiation + \$500/mo) launched in Feb. 2026.
- AI used “at every step of the attack chain”: chatbot analyzed victim inboxes, chose who to target and impersonate, and mapped payment-fraud strategies
- Used to gain access to email accounts through device-code attacks.
- Persistence via hidden inbox rules and newly registered devices; MFA defeated because the sign-in itself was genuine.
- ~1,000 criminal users; 12,000+ victim inboxes at 10,000+ orgs.
- 13+ correlated IC3 complaints (~\$1.7M losses).

CLAIMS & OUTCOME

- **Lanham Act §§ 1114, 1125** — counterfeit Microsoft marks in phishing emails and ads cause confusion and tarnishment.
- **ECPA § 2510 et seq.** — intercepted device codes; accessed customer Outlook email, incl. a Health-ISAC member.
- **CFAA § 1030** — unauthorized access to Azure and Health-ISAC member computers; transmitted damaging code.
- **RICO § 1962** — “EvilTokens Enterprise” engaging in wire fraud and criminal trademark infringement.
- **Tortious interference** — interfered with Microsoft’s contracts with Windows, Azure and Outlook customers.

OUTCOME

- 50 websites seized and 150+ associated domains disabled via court order.
- Two suspects arrested by the Met’s (UK) cybercrime team in Sept. 2026.
- Court case is ongoing.



OP. FAUX SIGN: CODE-SIGNING FRAUD

Microsoft Corp. v. John Doe 1 et al. | S.D.N.Y. No. 26-cv-03737 | Unsealed in May 2026 | Fox Tempest, Vanilla Tempest (VICE SPIDER)

THE SCHEME

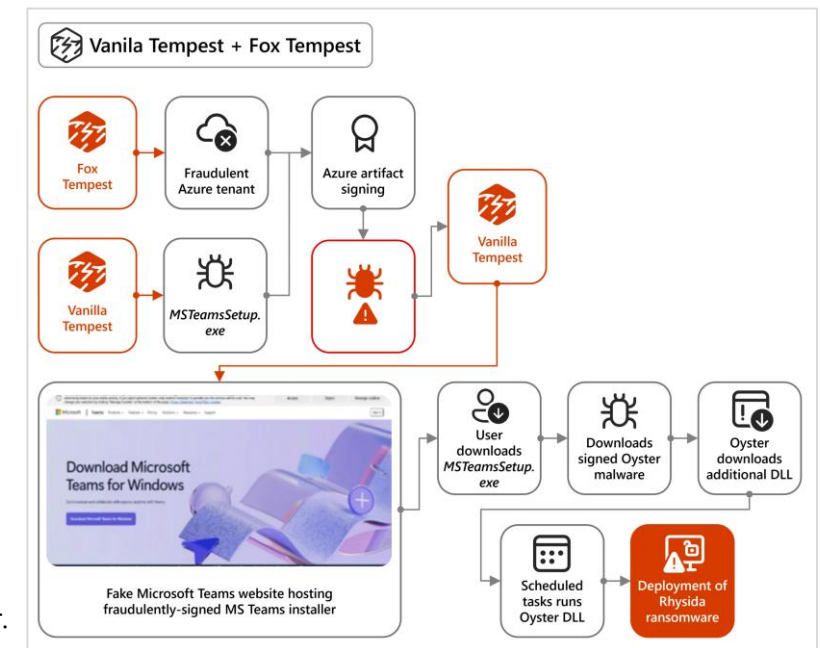
- Fox Tempest (active since May 2025): 580+ fraudulent Azure tenants used to obtain 72-hour code-signing certificates via Microsoft's Artifact Signing service.
- Access to code signing sold as a service for up to \$9,500; buyers incl. Vanilla Tempest (VICE SPIDER), Storm-0501, and Storm-2561.
- Customers could access the Fox Tempest-controlled tenants via virtual machines to sign their malware.
- Customer signed Rhysida ransomware, Oyster, Lumma Stealer and Vidar, disguised as Teams, AnyDesk, PuTTY and Webex installers.
- Resulted in cyberattacks against a broad range of industry sectors, including healthcare, education, government, and financial services, impacting organizations globally.

CLAIMS & OUTCOME

- **Breach of contract** — false ID/docs to create tenants; criminal resale.
- **Trespass to chattels** — unauthorized use of Artifact Signing.
- **Lanham Act § 1114, 1§ 1125** — malware passed off as Microsoft-signed and Microsoft marks used to disguise malware.
- **Unjust enrichment** — profits from ransomware and extortion.
- **RICO § 1962** — Fox Tempest (seller) + Vanilla Tempest (buyer).
- **CFAA §§ 1030(a)(6), (b)** — trafficking in fraudulent certificates; conspiracy to damage computers.

OUTCOME

- Signspace[.]cloud (hosting service) seized via court order.
- Hundreds of virtual machines taken offline via court order.
- 1,000+ fraudulent certificates revoked.
- Court case is ongoing.



STORM-2139: GENERATIVE AI ABUSE

Microsoft Corp. v. Yadegarnia et al. | E.D. Va. No. 1:24-cv-02323 | Default Judgment in July 2026 | Storm-2139

THE SCHEME

- Named defendants in Iran, U.K., Hong Kong and Vietnam abused Azure OpenAI Service with stolen customer API keys starting in July 2024.
- “Hacking-as-a-service”: the de3u tool let low-skill users generate DALL·E images with stolen keys.
- Reverse proxy routed traffic through a Cloudflare tunnel and stripped C2PA provenance metadata.
- Generative AI guardrails circumvented using custom tools sold to other cybercriminals; thousands of harmful images, incl. non-consensual inappropriate images of celebrities.

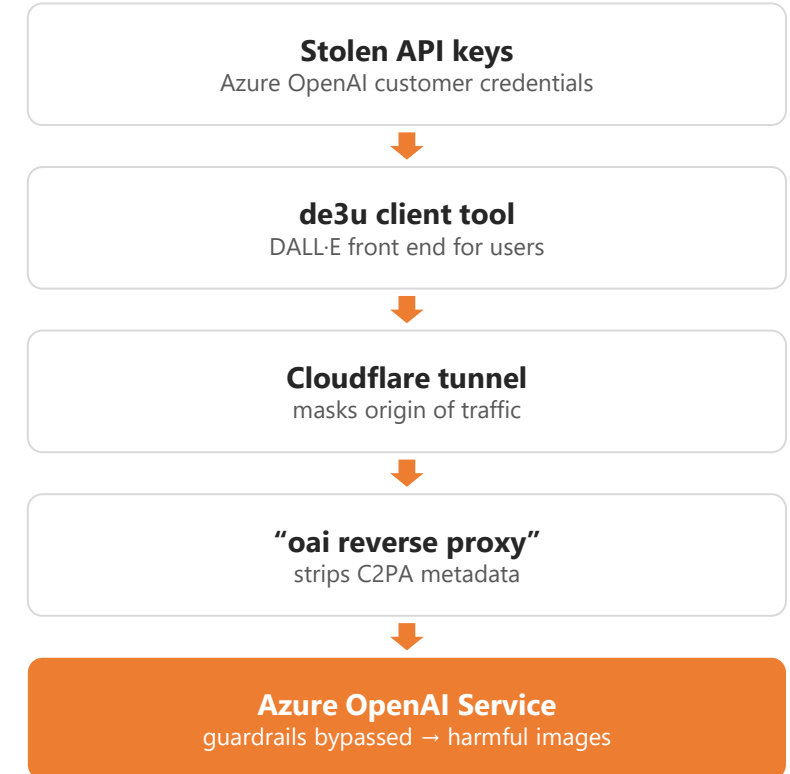
CLAIMS & OUTCOME

- **CFAA § 1030** — unauthorized Azure access.
- **DMCA § 1201(a)(1)** — circumvented access controls with stolen keys.
- **DMCA § 1201(a)(2)** — trafficked de3u and proxy tools.
- **Lanham Act § 1125** — distributed images containing Microsoft’s mark in metadata.
- **RICO § 1962(c)** — “Azure Abuse Enterprise” providing hacking-as-a-service software and infrastructure.
- **Trespass to chattels** — burdened Microsoft computers.
- **Tortious interference** — stole customer credentials and drained their accounts.

OUTCOME

- Seized domains associated with the service via court order.
- Default judgment awarded in July 2026.

HACKING-AS-A-SERVICE INFRASTRUCTURE



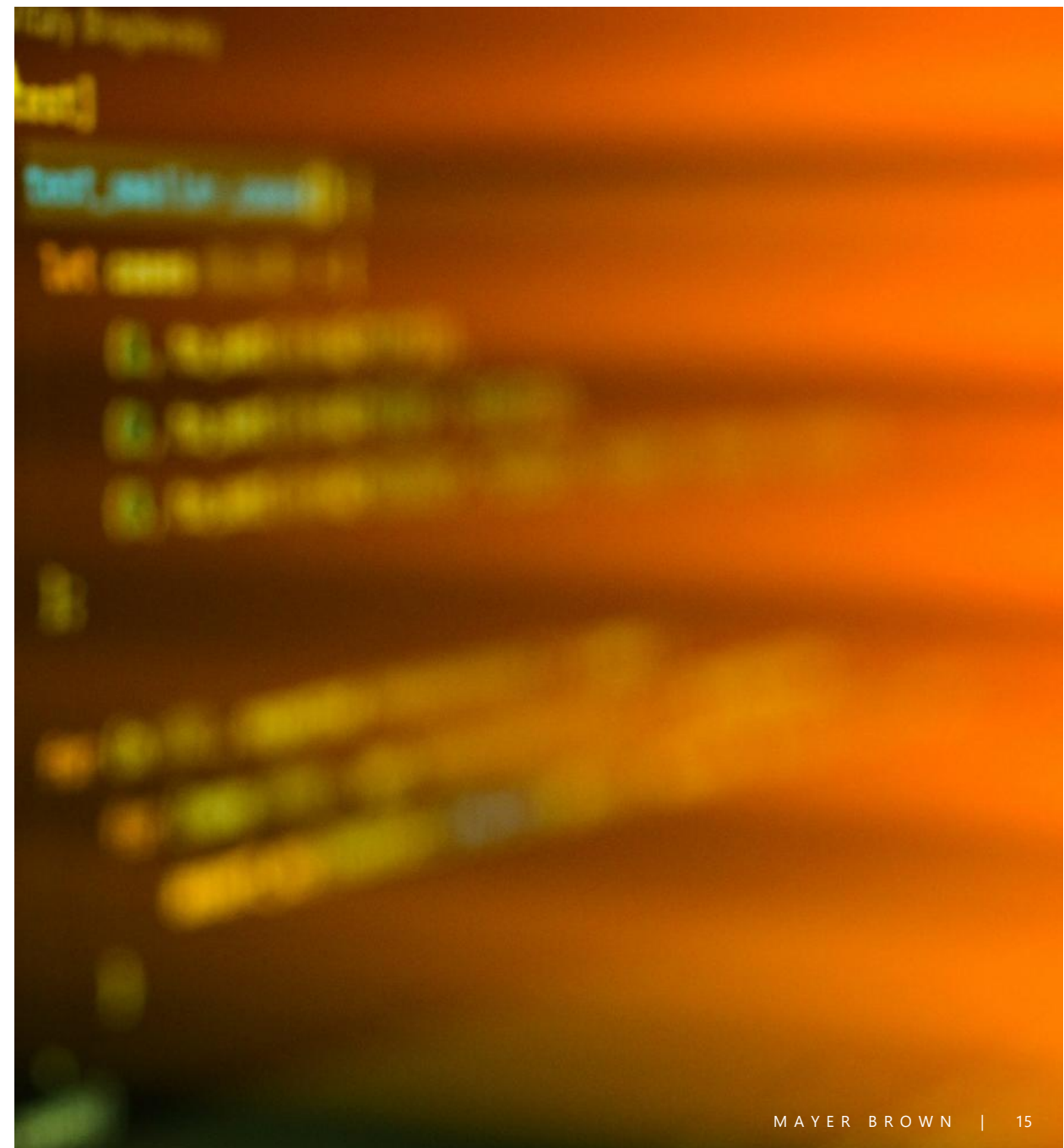
The background is a complex digital-themed abstract. It features glowing orange and yellow circuit traces on the left side, transitioning into a dark blue field with lighter blue circuit patterns. On the right, there are vertical columns of glowing blue binary code (0s and 1s). A thin white vertical line runs down the center of the image.

04

THEMES AND TAKEAWAYS

KEY TAKEAWAYS

- AI is a cybercrime enabler.
- Cybercrime is rented, not built — for a monthly fee, anyone can launch attacks.
- Cybercriminals often log in rather than break in.
- Companies can sue to take criminal websites offline, even before they know who is behind them.
- Old laws fit new crimes — traditional claims like breach of contract and trespass can be leveraged to fight cybercrime.
- Takedowns disrupt but don't completely end the threat — lasting impact takes law enforcement and industry working together.



“

Questions?

THANK YOU FOR JOINING US.



MAYER|BROWN

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global legal services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England & Wales), Mayer Brown Hong Kong LLP (a Hong Kong limited liability partnership) and Taill & Chequer Advogados (a Brazilian law partnership) (collectively, the "Mayer Brown Practices"). The Mayer Brown Practices are established in various jurisdictions and may be a legal person or a partnership. PK Wong LLC ("PKW") is the constituent Singapore law practice of our licensed joint law venture in Singapore, Mayer Brown PK Wong Pte. Ltd. More information about the individual Mayer Brown Practices and PKW can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown. © 2026 Mayer Brown. All rights reserved.