KROLL™

Threat Landscape Report:

Cybercrime in the Crypto Era

KROLL

Threat Landscape Report:

Cybercrime in the Crypto Era

Authors

The first half of 2025 saw the continuation of the complex themes that shaped the threat landscape in 2024. Email compromise retained its place as the most prominent threat type, while phishing continued to take the lead in initial access methods. Yet another trend that persisted was that of groups such as AKIRA, PLAY and LOCKBIT retaining their place as key ransomware players. However, alongside familiar threat types and players, risks associated with cryptocurrency proved to be a notable theme in Q1 2025, likely due to changing regulations and a rise in malware leveraging the blockchain. As a result, this report focuses on key findings and observations around cryptocurrency.

With significant potential rewards, cryptocurrency has become the focus for cyberattackers almost as fast as it has for investors. This presents some uniquely complex and unprecedented security risks. Political shifts have led to more giant leaps forward into the mainstream—further driving the scope for attacks. The Kroll Cyber Threat Intelligence team observed that nearly $1.93 billion was stolen in crypto-related crimes in the first half of 2025 alone, surpassing the total for 2024 and putting 2025 on track to be the worst year for digital asset theft. Additionally, phishing attacks targeting cryptocurrency users increased by 40%, primarily through fake exchange sites. These underscore the growing cybersecurity risks in the crypto space, from direct thefts and hacks to more sophisticated scams and laundering operations.

Continue reading for more insights into the cryptocurrency security risks shaping 2025 and the steps you can take to safeguard your organization.

The Changing Crypto Landscape: Political Shifts and Physical Threats

Crypto Kidnapping Attempts Accelerate

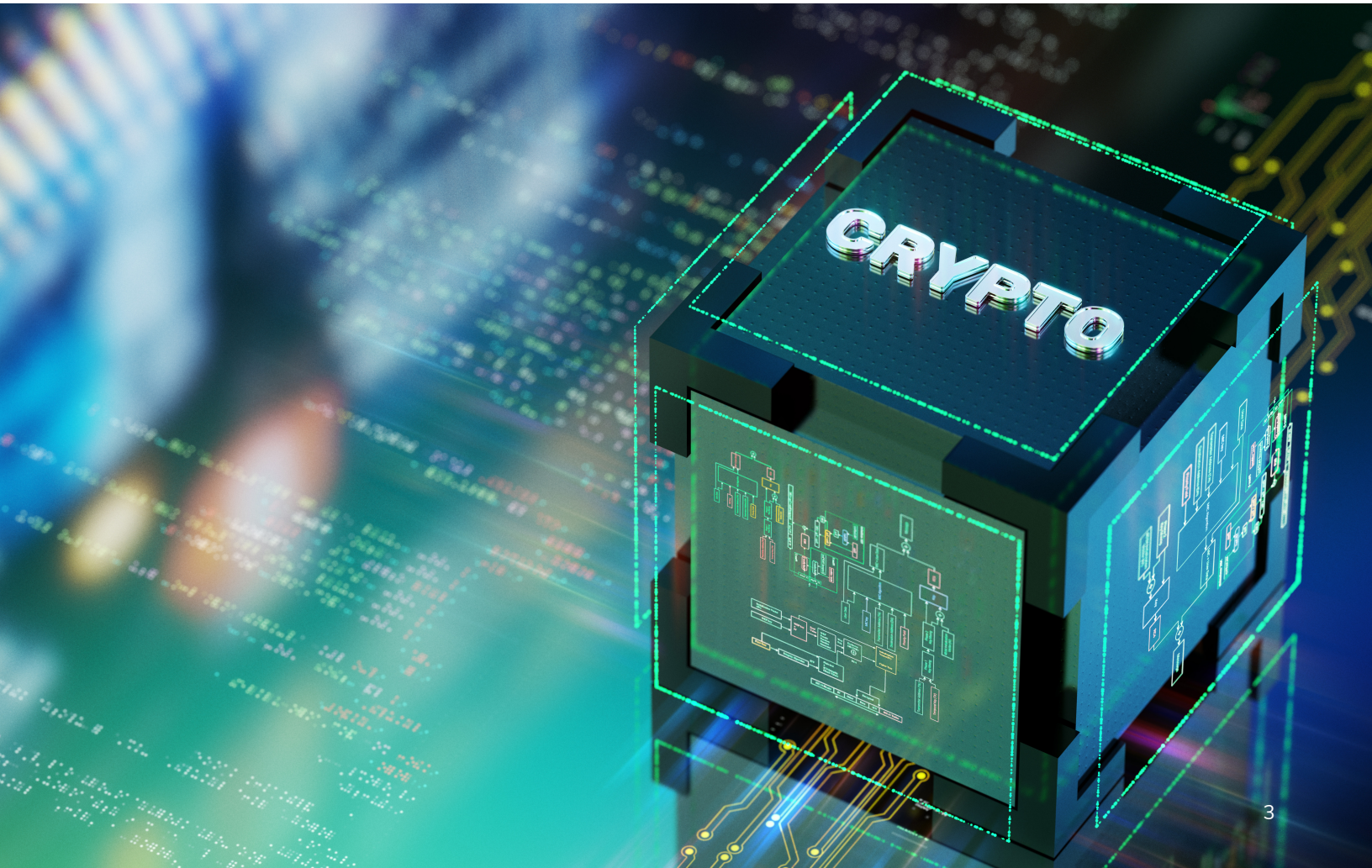
Crypto exchanges and financial organizations are becoming increasingly lucrative targets—not just for cyber threats but also for physical security threats—as their visibility and value continue to grow. The level of the physical risk now associated with crypto has been highlighted by recent kidnappings and ransom attempts, leading to a rise in investors seeking protection services, including bodyguards. Risks to companies also increase when they are only potentially exposed, as discovered in the May 7, 2025, LOCKBIT breach, where negotiation conversations were leaked, along with their Bitcoin wallet addresses.

Compliance Failures Drive Risk

Failure to establish compliance protocols for crypto services can expose financial institutions and organizations to serious legal repercussions, including fines, sanctions and reputational damage. In recent years, crypto services have garnered attention and a reputation as hubs for criminal activity, leading to stringent regulatory measures across various jurisdictions.

Poor Financial Insight Has a High Cost

Financial intelligence failures in the crypto industry can have disastrous real-world consequences. These include the financing of terrorist activities and enabling organized crime groups. Past crypto breaches highlight the concerns of digital assets causing financial turmoil across markets. For example, the Bybit breach coincided with the price of Bitcoin plunging by 20%.



KROLL

Achieving Crypto Compliance: Evolving Regulatory Requirements

Proving Compliance with Penetration Testing

Penetration testing (pen testing) is a crucial aspect of an organization's overall cybersecurity and compliance efforts, and serves dual purposes for crypto exchanges: first, by enhancing overall security posture and helping businesses meet compliance requirements set by various regulatory bodies. Secondly, documented penetration tests provide tangible evidence of an organization's commitment to security and compliance, which may be required during regulatory audits or assessments. While no single, universal law mandates pen testing, several regulations and frameworks require or strongly encourage it.

Regulations and Frameworks Requiring Penetration Testing

- Payment Card Industry Data Security Standard (PCI DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- General Data Protection Regulation (GDPR)
- International Organization for Standardization (ISO) 27001—the international standard which sets guidelines for Information Security Management Systems (ISMS)
- American Institute of CPAs (AICPA) SOC 2 Trust Services Criteria

Penetration testing is also relevant for compliance with other regulations and frameworks, such as those related to critical infrastructure and government systems. Penetration testing regulations for cryptocurrency businesses are primarily focused on ensuring security, complying with regulations and protecting user assets.

Crypto Oversight: Charting the Regulatory Landscape

The U.S. and EU have two separate characteristics in relation to crypto risk; where the U.S. relies on existing securities laws and enforcement actions to address them, the EU framework is intended to provide a well-coordinated regulatory framework for crypto assets for all EU member states.

Crypto in the U.S.: Robust Security Testing Required

In the U.S., January 2025 saw President Donald Trump issuing an executive order declaring crypto a national priority and supporting "the responsible growth and use of digital assets, blockchain technology and related technologies across all sectors of the economy."

A fundamental regulatory point being addressed is whether cryptocurrency should be regulated by the SEC as a security or by the Commodity Futures Trading Commission as a commodity. Several bills are under consideration in Congress, including the Clarity for Payment Stablecoins Act and the Lummis-Gillibrand Payment Stablecoin Act.

The Financial Crimes Enforcement Network (FinCEN) stipulates that exchanges must implement comprehensive security measures that include penetration testing as part of their compliance with the Bank Secrecy Act (BSA). Crypto exchanges that process credit card payments must also adhere to requirement 11 of Payment Card Industry (PCI) Data Security Standard (DSS) 3.2.1, which specifically mandates regular penetration testing. The SEC treats many cryptocurrencies as securities and is concerned with investor protection. While not explicitly requiring penetration testing, it does require financial institutions to have robust security testing to ensure compliance. The testing could be used to identify potential vulnerabilities that could be exploited by threat actors.

Crypto in the UK: Seeking a Balanced Regime

In December 2024, the UK's Financial Conduct Authority (FCA) published a Discussion Paper (DP) titled DP24/4: Regulating Cryptoassets—Admissions & Disclosures and Market Abuse Regime for Cryptoassets. In keeping with the FCA's latest five-year strategy, it is keen to introduce a balanced regime which supports growth in the UK. To this end, the focus of DP 24/4 is spot cryptoassets, such as stablecoins, and what the FCA refers to as unbacked cryptoassets (e.g., bitcoin). It does not include those already captured under the existing list of specified investments in Part III of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, such as tokenized financial instruments. The FCA published DP23/4 to help develop the UK's regime for fiat-backed stablecoins. This is part of a series of publications by the FCA designed to facilitate the development of the UK's cryptoasset regulatory regime.

Crypto in the EU: DORA Sets Out Need for Threat-Led Pen Testing

The Digital Operational Resilience Act (DORA) applies to a wide range of financial entities, including crypto-asset service providers and issuers of crypto-assets. DORA requires relevant organizations in the EU to carry out controlled assessments—Threat-Led Penetration Tests (TLPTs)—of their cyber resiliency on a regular basis. This involves an intelligence-led approach to classic red team testing that targets an organization's most critical business systems.

Articles 25-27 stipulate that TLPTs take place against IT assets:

- Supporting "critical or important functions" of a financial entity (including third-party systems if/as appropriate).
- Using real-world tactics, techniques and procedures (TTPs) obtained via tailored threat intelligence analysis.
- To proactively identify—and allow entities to swiftly mitigate/remediate—any weaknesses, deficiencies or gaps in their implementation of controls and counteractive measures.

TLPTs must be performed at least every three years if an organization is deemed in scope by the supervising authorities. Finally, TLPTs for DORA should be followed in accordance with the preexisting Threat Intelligence-Based Ethical Red-Teaming (TIBER)-EU framework, with some additional considerations and aspects now also formalized and included in DORA, such as now mandatory purple team exercises.

KROLL

Taking a Bite out of Bybit: A Timeline of the World's Biggest Crypto Hack

February 21: Threat Actors Hit Bybit

Cryptocurrency exchange Bybit discloses the theft of more than $1.46 billion worth of cryptocurrency from one of its cold wallets in the largest cryptocurrency hack ever, almost doubling the $620 million stolen from Sky Mavis in March 2022. It is thought that this money is used to directly fund the North Korean government.

February 23: Attribution to Lazarus

Confirmation of analysis of the hack attributes it to the North Korean-linked Lazarus Group (KTA071), revealing the commingling of funds from the initial Bybit theft address and BingX, and Phemex exploits previously attributed to the group.

Blockchain analysis firm Chainalysis reports on the attack in further detail and also notes consistencies between the actors' TTP and those of North Korean threat actors, aligning with other research entities where KTA071 (Lazarus) has been attributed. This attribution was also stated by Safe, which manages the smart contracts system that was targeted.

February 26: Confirmation by FBI

The FBI announces that North Korea was responsible for the attack.

April: **Leveraging LinkedIn**

A campaign is discovered that sees a continuation of the group's commonly used initial access method through the impersonation of recruiters on LinkedIn.

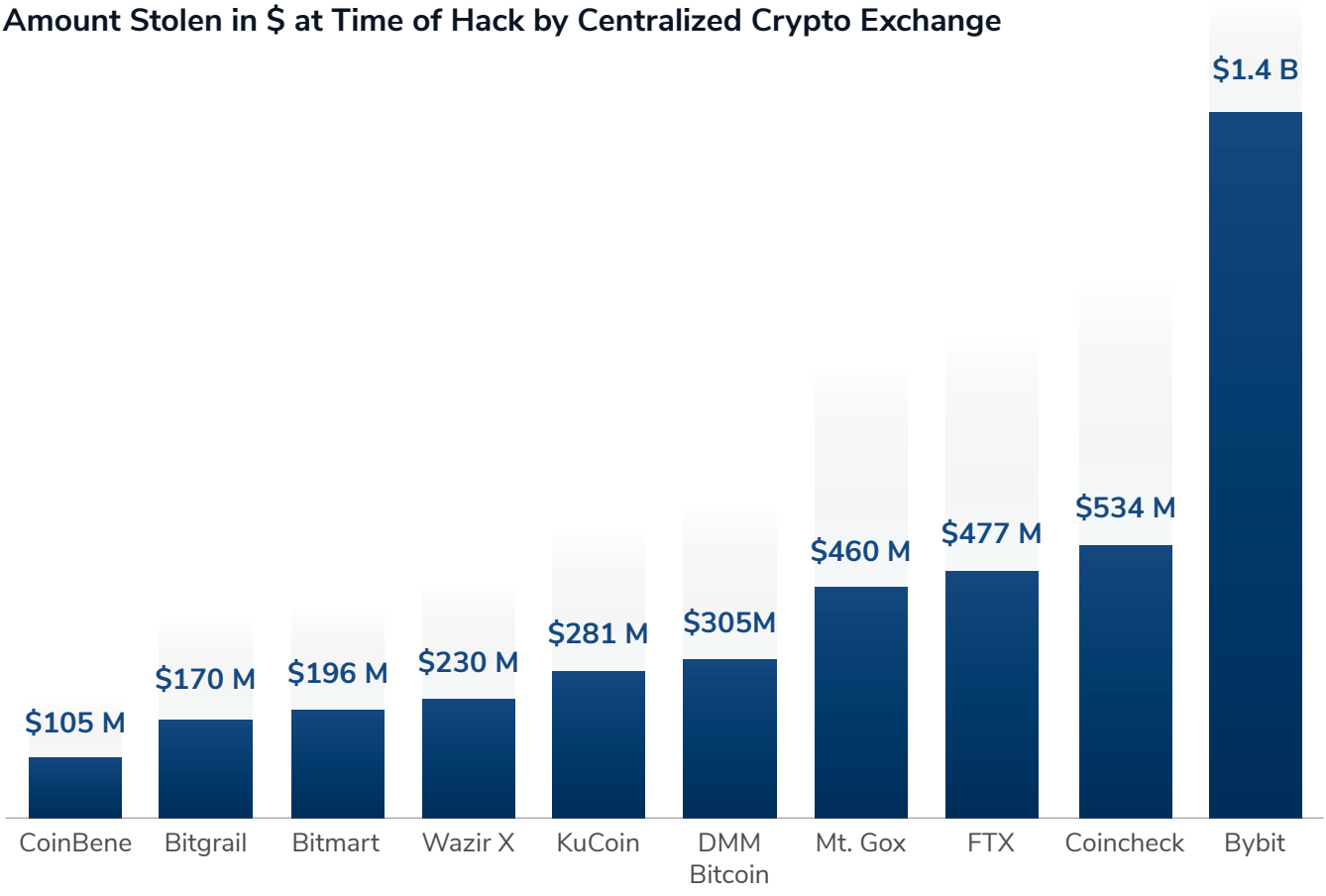
The PDF lures sent to applicants via LinkedIn include a coding challenge. The script's function is to load and execute the first malicious payload by creating a blank Python file in the "/Public/" directory and writing decoded base64 data to it. This new file is identified as RNLOADER, which in turn downloads and executes RNSTEALER, which is the main malicious payload observed in the report.

The purpose of RNSTEALER is similar to other information stealers in gathering basic victim information, file and directory listings, as well as stored keys for Secure Shell (SSH), Amazon Web Services (AWS), Kubernetes and Google Cloud. From here, the threat actor will likely assess the stolen information and whether more activity, such as persistence, is needed for that victim, which could be used for pivoting to more important corporate assets.

Current: **Changing Behavior**

Kroll believes that KTA071 is also now also leveraging the ClickFix technique as part of its attack chain.

Amount Stolen in $ at Time of Hack by Centralized Crypto Exchange



Source: The 10 Biggest Crypto Hacks in History

KROLL

The Malware Spotlight

Malware Trends Analysis

Q1 2025 Trend	Threat Name
→ 1	LUMMASTEALER
↑ 2	CLEARFAKE
↓ 3	STEALC
↑ 4	IDATLOADER
↑ 5	ASYNCRAT
→ 6	XWORM
↓ 7	AGENTTESLA
→ 8	AMADEY
↑ 9	GOOTLOADER
↑ 10	FULLMETAL

Malware trends for Q1 2025 feature persistent threats, heavy hitters and some newcomers, such as FULLMETAL, which stemmed from the PDFast software being hit with a supply chain attack, which then dropped to malware. This is a particularly notable case because PDFast and similar types of threats such as Chrome extensions, discussed in previous reports, impact a large number of organizations at the same time. The Kroll Cyber Threat Intelligence team has seen evidence that there are still some infected versions of PDFast out there.

The rest of the top ten reflects trends observed since at least early to mid-2024: many information stealers and a lot of malware that is designed to target identity, a key concern.

While the Cyber Threat Intelligence team saw far less of the “land and expand” methodology—where threat actors land malware and then other custom malware spreads into the rest of the organization—they did observe a lot more “malware-less attacks” that mainly involve living off the land binaries and deployment of information stealers.

CLEARFAKE: Powered by Blockchain

Kroll continues to observe widespread attempted initial access through CLEARFAKE via fake CAPTCHA pop-ups across a wide range of industry sectors.

CLEARFAKE is a malicious in-browser JavaScript framework deployed on compromised webpages as part of drive-by compromise campaigns. Its use has impacted thousands of people since it was first identified in 2023.

Current Status: Although CLEARFAKE continues to show the same themes surrounding its use alongside fake CAPTCHA pop-ups, a wide range of nuances that have appeared in the Q1 2025 highlight the swift development of CLEARFAKE-related compromises across clusters of activity within Kroll data.

Discover further insights from Kroll on the rapid evolution of CLEARFAKE delivery.

CLEARFAKE and EtherHiding

CLEARFAKE uses the "EtherHiding" technique to store malicious payloads on the blockchain. EtherHiding is a technique that allows near permanent hosting of malicious logic on a blockchain as a ledger entry, enabling a malicious actor to rely on the retrieval, delivery and execution of the malicious JavaScript indefinitely. It works by taking advantage of certain blockchain characteristics, such as immutability and peer-to-peer distribution.

On a blockchain ledger, each entry is a "block" containing the hash identifier of the previous block as well as transaction data. This daisy-chains together a transaction history, and any attempts to modify these transactions will cause previous hash identifiers to be invalid and therefore fail calculation.

Changes to the blockchain therefore require rolling back all transactions, and due to the frequent peer-to-peer nature of the technology, ledgers are difficult to remove or take down. Transaction data can vary and, in the case of EtherHiding, is composed of a "smart contract." This can be thought of as logic that will execute to fulfill terms of a contract when the contract conditions are met.

The Weakest Link: The CLEARFAKE EtherHiding Blockchain Technique

User Browses Compromised Web Page

The CLEARFAKE campaign begins with a user browsing to a compromised webpage, typically a WordPress site, acting as a drive-by compromise waiting for users to land on the page. The technique of fetching and presenting the fake updates prompt involves using Ethers, a JavaScript library alongside BNB Smart Chain (BSC), the smart contact system for the BNB cryptocurrency that was created by Binance.

Malicious Code Stored

The threat actor stores a contract object that contains the malicious code on the BSC and allows for programmatical retrieval via the Binance endpoint.

JavaScript Function Embedded

The threat actor embeds a simple JavaScript function on the compromised website (usually in a template that would get loaded by all pages).

Copy of Object Obtained

This code uses the Ethers library to obtain a copy of this object from the BSC, which the threat actor treats as code and runs with the JavaScript.

POST Request Initiated

Once the request is made using the Ethers library, the victim's browser initiates a POST request to the BSC using JSON-RPC with the following response format with an encoded string at the end (truncated for ease of viewing): "{"jsonrpc":"2.0","id":44,"result":"0x000000000000000[....]"

Mission Accomplished

The response format contains the actor-controlled domain address for the delivery of the payload that identifies and executes on the browser, displaying the correct language and fake browser iframe to the victim.

Case Study: Havoc Reigns After Major Cryptocurrency Theft

Key Findings

Kroll researchers discovered two new pieces of malware, a backdoor and a loader named “PRELUDE” and “DELPHYS,” respectively.

This malware led to deployment of Havoc C2’s agent, “Demon,” while investigating a large-scale cryptocurrency theft.

Havoc C2 is an open-source, post-exploitation command and control framework.

Challenge

During the investigation of a large-scale cryptocurrency theft, with total losses significantly exceeding $1 million spread across multiple currencies, Kroll researchers discovered two new pieces of malware. These pieces of malware ultimately led to deployment of Havoc C2’s agent, “Demon.” Kroll believes the threat actor was targeting individuals of high net worth in the cryptocurrency space.

Impact

Once Demon is installed and running on the system, the threat actor has access to a wide set of features, giving them all the access they need over the victim’s machine to realize their theft. Kroll found two pieces of malware we believe had not been previously documented, a backdoor and a loader we named “PRELUDE” and “DELPHYS,” respectively.

Learn More

Read more about how the Kroll Cyber Threat Intelligence team handled this case here.

KROLL

Navigating the Crypto Gold Rush: All That Glitters Is Not Gold

Political and cultural changes mean that the cryptocurrency ecosphere offers a new frontier for investors, businesses and cybercriminals alike. Trends observed by our Cyber Threat Intelligence team in Q1 2025 demonstrate that while the concept of crypto isn't exactly new, its continued development and move to the mainstream mean that it poses some very new and very real threats to both financial services companies and businesses seeking to evolve the way they transact with customers. From information stealing to malware to social engineering, patterns noted by Kroll in 2025 highlight that all organizations need to stay vigilant about the potential of attacks that focus on obtaining cryptocurrency or leveraging its vulnerabilities.

Kroll's Cyber Threat Intelligence team recommends the following steps:

Address the Essentials

Avoid giving attackers an easy way in by ensuring that your core security controls are addressed. This means ensuring all staff use strong passwords (particularly those linked to cryptocurrency wallets) and enforcing the use of multifactor authentication. Alongside this, implement regular security awareness and training.

Audit, Assess, Review

Security audits provide critical insight into the wider resilience of your organization. Rather than relying on one-off security checks, establish a regular program of audits to identify vulnerabilities and test the limits of your cybersecurity defenses. With physical attacks associated with crypto now ramping up, organizations should review their physical safety measures as soon as possible, both on an organizational and an individual level.

Keep Private Keys... Private

The security of private cryptocurrency wallet keys is critical. Ensure they are stored and safeguarded using secure methods, such as encryption and hardware wallets.

Act Fast

In the event of an attack, it is critical to take effective action to mitigate and minimize the impact on your assets and reputation. Organizations can ensure this by collaborating with a trusted security partner who has a proven track record for enabling crypto companies, investors and law enforcement to meet their most critical challenges, as well as a focus on investigating and remediating at pace.

Get Ahead of Regulatory Requirements

Responding to the changing crypto threat also involves the ability to keep pace with changing rules and regulations; developing robust governance; establishing risk and compliance frameworks; implementing effective anti-money laundering, sanctions and market surveillance programs; and preparing for compliance with incoming digital asset regulations.

It is critically important for companies using crypto globally to be aware of individual country regulations so they are not in violation of global financial system regulations or other countries' integration and regulation policies. Again, expert advice from a trusted partner can ensure that effective arrangements and documentation are in place to meet regulatory expectations and progress at pace through remediation and regulatory scrutiny.

Apply Customer Intelligence

A key defense against crypto-related threats is current and precise insight into the people and companies your organization is seeking to work with. The most effective actionable intelligence for compliance among organizations and institutions is to thoroughly know their customers. This involves implementing robust Know Your Customer procedures to verify the identities of clients, understand their financial activities and assess potential risks. Overall, organizations must take proactive and preventive intelligence actions to avoid damages.

Look out for the Big Phish

With phishing a key weapon for crypto scammers, ensure that employees are vigilant about all types of unsolicited emails, especially those related to cryptocurrency.

Stay Ahead of Threats with Expert Guidance

The Challenge of Navigating Persistent, Complex Conditions

As organizations navigate recurring and fluctuating risks to their cybersecurity posture and critical data, such as persistent cyberattacks, evolving compliance requirements, complex supply chains and emerging technology vulnerabilities, there needs to be sustainable processes in place to continuously anticipate, withstand, and recover from these adverse conditions.

Kroll is your go-to partner for simplifying the complexity of cyber and data resilience

We provide reactive, advisory, transformation and managed security services to support clients at every stage of their resilience maturity.

Our services leverage frontline risk intelligence from thousands of incident response, regulatory response, financial crime and M&A due diligence engagements per year to anticipate the most likely risks to your business and reduce your unique threat profile.

We combine this with over 650+ experts with background experience in law enforcement, industry and regulatory agencies to help you establish efficient, sustainable solutions to complex and persistent cyber and data resilience issues.

Our Credentials

World's largest IR provider with 1000+ IR cases a year

Highly rated by industry analysts in IR, MDR, Security Consulting and GRC

Forrester IDC GIGAOM

100+ certifications

CISM CREST ISO 27001 Cyber Essentials Certified Plus CISSP ISSAP

Expertise with **leading vendors**

CrowdStrike DARKTRACE LogRhythm Microsoft paloalto NETWORKS
Qualys. tenable SentinelOne splunk> FLASHPOINT
vmware Carbon Black INTEL471 FRAUDWATCH Meltwater Relativity
Agiloft reveal OBSIDIAN integreon

Kroll Cyber and Data Resilience Services

React	Advise	Transform	Operate
Incident Response & Recovery	Security Assessments & Advisory	Cloud & Application Security	Managed Detection and Response
Breach Notification	Penetration Testing & Red Teaming	Technology Implementation (IAM, Threat & Vulnerability Management, OT Security etc.)	Digital Risk Protection
Data Discovery & Management	AI Risk Management	Security Program Development	Security Technology & Process Management (OT, IAM, AI etc.)
Expert Witness & Litigation Advisory	Regulatory Compliance Assessments	Zero Trust Security	Fraud Detection and Prevention
Cyber Due Diligence	Financial Crime Compliance & Investigations	Cyber Security Training	Corporate Legal Operations

Kroll Risk Intelligence

Frontline intelligence from thousands of IR, regulatory response, financial crime, and M&A due diligence engagements a year

KROLL™

TALK TO A KROLL EXPERT TODAY

North America
T: 877 300 6816

UK
T: 808 101 2168

Hong Kong
T: 800 908 015

Additional hotlines at:
kroll.com/hotlines

Singapore
T: 800 101 3633

Australia
T: 1800 870 399

Brazil
T: 0800 761 2318

Or via email:
CyberResponse@kroll.com

Browse the latest editions of Kroll's Quarterly *Threat Landscape* reports and subscribe for free at **kroll.com/cyberblog.**

About Kroll

As the leading independent provider of financial and risk advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.