
ncc group
FOX IT
part of ncc group
Cyber Threat Intelligence Report
Review of May 2026

Contents

Section 1
Executive summary

For May 2026, ransomware activity plateaued, with 749 victim listings recorded, reinforcing the elevated baseline observed throughout 2026. The Industrials sector remained the most frequently targeted, with activity levels broadly consistent with previous reporting periods. Qilin continues to hold its position as the most prolific ransomware operation by volume, while The Gentlemen group ranked second for the second consecutive month. Although relatively new, The Gentlemen's sustained level of activity suggests it is establishing a notable presence within the current ransomware landscape.

This month's Ransomware spotlight discusses the implications of the convergence between nation-state and cybercriminal operations, following the reported discovery of a MuddyWater campaign disguised as Chaos ransomware. Recent reporting indicates that Iranian threat actors are leveraging ransomware ecosystems alongside criminal infrastructure and tooling to complicate attribution and increase operational flexibility. As the distinction between cybercrime and state-sponsored activity erodes, defenders should prepare for hybrid threats by improving situational awareness and prioritising behaviours over indicators.

The Geopolitical developments section of the May Pulse examines the implications of major geopolitical events during the reporting period. While Russia remains an unpredictable threat to European security, China's growing assertiveness is likely to elevate cyber risk globally. Strategic competition between China and the United States and its Quad partners may drive more threat activity from China-aligned actors. To support broader state-backed strategic objectives, China-affiliated groups may seek strategic intelligence, maintain access to priority targets, and shape political narratives.

With the growing weaponisation of artificial intelligence, this month's Emerging cyber security trends examines Kitana, a purpose-built Adversary-in-the-Middle (AiTM) fraud platform identified by NCC Group. Kitana demonstrates how AI-assisted development is accelerating cybercriminal tooling while lowering entry barriers. As AI reduces the cost and complexity of developing attack frameworks, organisations should anticipate a more capable and rapidly evolving fraud ecosystem. Domain infrastructure monitoring and improved user awareness are critical measures for strengthening organisational resilience.

Section 2

Ransomware key statistics: May 2026

4%

Global ransomware attacks decreased by 4% in May 2026

29%

Industrials accounted for 29% of ransomware attacks in May 2026

15%

Qilin was responsible for 15% of attacks in May 2026

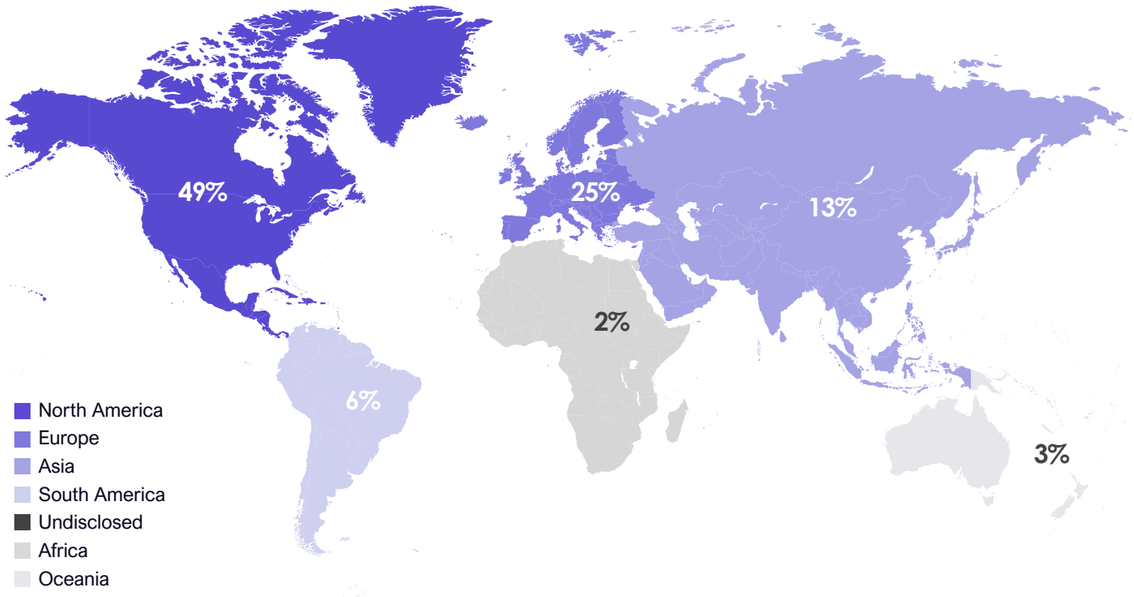


Figure 1: Ransomware attacks by region, May 2026

NCC Group can support you in mitigating ransomware threats.
Please see our contact details at the end of this report, should you require assistance.

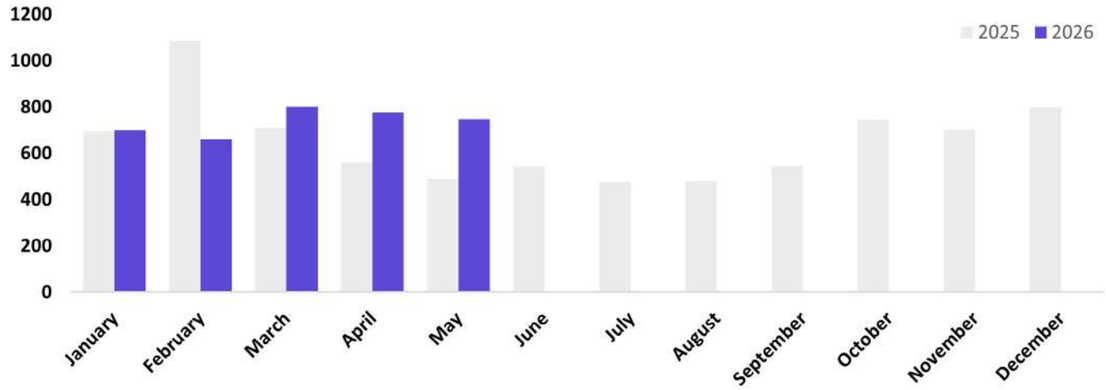


Figure 2: Ransomware attacks by month 2025 - 2026

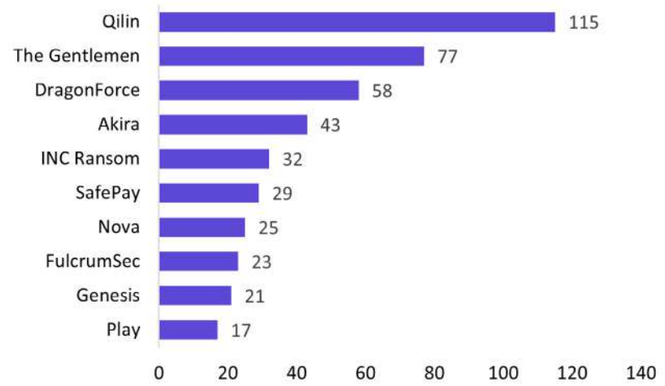


Figure 3: Top threat actors, May 2026

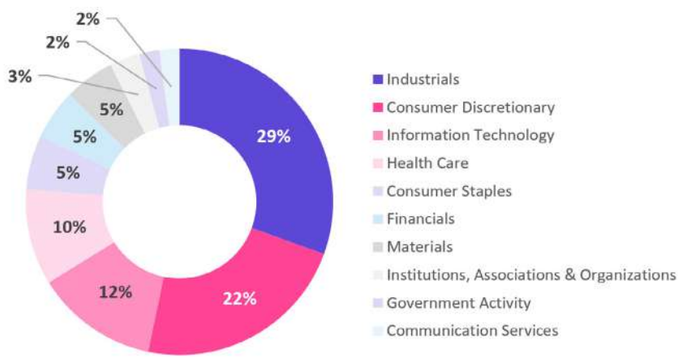


Figure 4: Top targeted sectors, May 2026

Key events

04/05/2026
West Pharmaceutical Services

West Pharmaceutical Services suffered a ransomware attack on 4th May, leading to shutdown of affected systems and global operational disruption. Data was exfiltrated before encryption, and while core systems and some operations are restored, full recovery is ongoing and the extent of data impact remains unknown.

11/05/2026
Foxconn

Foxconn confirmed a cyberattack affecting its North American operations, with production now recovering. The Nitrogen ransomware group claims it stole 8 TB of data, including millions of sensitive files such as internal documents and technical project details involving major firms like Apple, Nvidia, and Intel.

15/05/2026
Grafana

Grafana confirmed a breach caused by a compromised token that gave attackers access to its GitHub, allowing them to download source code. No customer or personal data was affected, systems remain secure, and Grafana refused to pay the ransom while continuing its investigation.

Section 3

Ransomware spotlight: The growing convergence of state and criminal cyber operations

On 6th May, Rapid7 published a report detailing a 'false flag' espionage campaign attributed with moderate confidence to MuddyWater (also known as Seedworm, Static Kitten, Mango Sandstorm, Mercury, TEMP.Zagros, TA450, and Earth Vetala).[1] MuddyWater is a cyber espionage group assessed to operate as a subordinate element of Iran's Ministry of Intelligence and Security (MOIS). Active since at least 2017, the group has targeted a broad range of government and private-sector organisations across multiple regions and industries.[2] According to the report, MuddyWater posed as Chaos ransomware to disguise their targeted state-backed activity as opportunistic cyber extortion.

The Chaos incident is not the first instance of MuddyWater disguising its operations as a ransomware activity. The adoption of criminal personas and ransomware branding by Iranian threat actors, including MuddyWater, is a well-documented practice; however, in this incident, the group expanded upon this approach.

Rather than relying solely on branding, the MuddyWater operators incorporated extortion notes, victim negotiation channels, and a listing on the Chaos leak site to reinforce a more persuasive appearance of a financially motivated intrusion. These measures suggest a deliberate effort to support the ransomware narrative, demonstrating how MuddyWater continues to adapt its deception techniques.

MuddyWater-ransomware links: from mimicking to integration

Nation-state threat actors, including Iran-nexus, are increasingly leveraging criminal infrastructure, tradecraft, tooling, and branding to shape initial perceptions of their operations. The MuddyWater-Chaos case is another example of a broader hybridisation trend that has become more pronounced in recent years. Earlier manifestations of this pattern were documented between 2020 and 2021, when some Iranian threat actors, including MuddyWater, reportedly disguised destructive wipers as ransomware attacks.[3]

In a 2020 campaign targeting Israeli entities, MuddyWater attempted to install a variant of 'PowGoop', a malicious replacement for the Google Update DLL.[4]

In 2024, a shift was observed when some Iranian operators began directly participating in cybercrime economies rather than mimicking cybercriminals.[5] Over the past year, reporting has highlighted the growing overlap between state-sponsored operations and cybercriminal activity across multiple Iran-linked groups. Reporting in 2026 indicates that several Iran-linked threat actors are increasingly leveraging cybercriminal operational models, off-the-shelf tooling, and cybercrime-related infrastructure in support of state-backed objectives. The trend is particularly evident among MOIS-linked groups, including Handala Hack and MuddyWater, whose operations have demonstrated repeated overlap with criminal tooling and infrastructure.[6] Beyond flexibility, this operational fusion is intended to provide plausible deniability and misdirect defensive efforts.

More broadly, this trend challenges a long-standing assumption that distinguishes financially motivated cybercrime from nation-state activity as separate threat categories requiring different defensive models. Several security vendors have characterised the convergence of these traditionally discrete threat ecosystems as a defining feature of the 2026 cyber threat landscape.

Numerous campaigns proved exceptionally difficult to attribute, with criminal groups adopting nation-state tradecraft, state-backed actors conducting operations indistinguishable from cybercrime, and governments leveraging cybercriminal services. Cyble recently reported tracking numerous campaigns "where attribution became nearly impossible".[7]

Recommendations

The findings outlined above highlight the need for organisations to reassess how ransomware incidents are interpreted and investigated.

Defenders should avoid automatically assuming that a ransomware incident is solely financially motivated. Such activity may represent conventional criminal extortion, an attempt to obscure an intelligence-gathering operation, a collaborative arrangement, or a disruptive campaign disguised as ransomware. Going forward, organisations and defenders should therefore move beyond treating ransomware and state-sponsored intrusions as inherently separate threat categories.

One of the key implications of this evolving state-criminal overlap is that defenders face growing uncertainty around escalation and stakeholder engagement decisions. Knowing when and whether to involve external parties becomes more difficult when attribution is delayed or contested. As the distinction between criminal and state-sponsored activity continues to blur, organisations should adopt defensive processes capable of operating effectively under conditions of attribution uncertainty. Mature defensive strategies should prioritise behavioural analysis, operational context, observed tradecraft, and adversary objectives over signature-based artefacts.

Static indicators may be shared or deliberately planted to mislead defenders, reducing their reliability as evidence of attribution or intent.

Final thoughts

MuddyWater is no longer relying on pseudo-ransomware operations or wiper-disguised-as-ransomware campaigns. Instead, the group appears to be participating in, or impersonating affiliates of, established criminal RaaS operations such as Qilin and Chaos. Following reports linking Iranian groups to these operations, it is likely that they will continue to leverage established criminal ecosystems and ransomware brands in the short-to-medium term. This approach may enable state-directed activity to blend more into the broader cybercriminal landscape, making such operations more difficult to distinguish from conventional financially motivated campaigns.

Section 4
Geopolitical developments

NCC Group's Threat Intelligence Team highlight geopolitical developments from the month which have the capacity to influence the cyber threat landscape.

14/05/2026

Between 14th and 20th May Chinese leader Xi Jinping hosted both US President Donald Trump and Russian President Vladimir Putin in successive, separate visits to China.[8] The 2-day US trip - the first by a US President since 2017 and also made by President Trump - ended on 15th May, with relatively modest trade developments, an announced framework to work towards 'reciprocal tariff reduction', and an invitation for Xi to visit the US later this year.[9]

Whilst President Trump appeared careful to avoid exacerbating geopolitical tension with China during the visit, Xi reportedly warned of US interference over Taiwan risking conflict, and publicly reframed a description of their relationship as seeking "constructive strategic stability". On 20th May, during a summit with President Putin, China highlighted multiple areas where China is aligned with Russia but critical of the US; specifically, President Trump's planned Golden Dome missile defence shield and failure to maintain a nuclear treaty with Russia.[10] Additional critical public comments were made without naming the US explicitly, for example, contrasting 'unilateral hegemonic currents [which] are running rampant' with Russian-Chinese efforts described as 'the main stabilising factor on the international stage'.[11]

So what?

- Whilst the US choice to take a delegation of prominent private sector leaders can be interpreted as an indication of prioritisation of economic interests over national and global security, broader actions by the US government in recent months publicly acknowledge the active Chinese security threat.[12,13] For example, this includes reporting on intelligence sharing with Iran during the ongoing conflict, IP theft, and insider threats.[14] The tension between economic and security interests, which creates a fragile geopolitical situation and a constant threat of escalation, is not limited to US relations with China and underpins a strong driver within the global cyber threat landscape. Intelligence agencies and nations with cyber capabilities seek advantage to navigate this tension; acquiring access to information, shaping narratives and exerting influence beyond public statements and activities, and pre-positioning destructive capabilities as an insurance policy against future conflict. Organisations operating at the intersection of tension points, or within wider national communications infrastructure, remain at high risk of network compromise and layered approaches to persistence and data exfiltration.
- As the Chinese threat to US strategic interests persists, the lack of visible efforts to induce or encourage shifts in China's approach suggests a recognition of a shifting balance of power between the two countries, and a related lack of capability to create change without risking intolerable harm to US interests.[15] Some analysts attribute this (at least partially) to a current period of unprecedented vulnerability for the US. It is difficult to avoid interpreting current events as an indication of China's rising level of global confidence and sense of opportunity. Related risks include potential changes to Chinese cost-benefit calculations over using cyber capabilities in pursuit of strategic goals. Chinese risk tolerance for discovery or attribution may increase and lower the threshold for cyber espionage and data theft. In parallel, the proven risks from the threat of an unpredictable and volatile US leadership may increase China's perceived need for 'just-in-case' leverage, such as pre-positioning. These factors are assessed as increasing overall risk levels of existing threats from Chinese nation-state threat actors and malicious insiders for both US organisations, and organisations involved in international responses to shifting global powers.
- The timing and nature of China's summit with Russia are consistent with a demonstration of defiance to the global community. The lack of significant new wins for Russia (specifically a new energy pipeline agreement) indicates that China is also confident in exercising dominance over its relationship with Russia, and that the relationship is limited by practical, mutual benefit rather than an ideological alliance. This creates a benefit for China in maintaining strategic advantage over Russia, and lowers the risk of true collaborative cyber activities and knowledge transfer between Chinese and Russian nation-state threat actors; suggesting that defenders should maintain awareness and robust defensive posture against the distinct threats each country represents.

25/05/2026

An expert report published on 25th May and wider media reporting suggest that the 'positional' phase of the ongoing war in Ukraine observed since 2023 is being replaced by relative Ukrainian advantage.[16,17] Whilst neither side is assessed as currently capable of conducting true operational manoeuvres, Ukraine appears to have secured some current tactical advantages, including drone supremacy, deep strike capabilities, recent successes with mechanised equipment on the front lines, and a net gain of territory for the first time since 2023. Long-term investments in Ukrainian command and control, alongside the cumulative impact on Russian military, logistics, and economic infrastructure, may now be contributing to Ukraine's capabilities. In 2026, Russian rate of advancement has dropped to low levels whilst casualty rates increase and the number of Russian soldiers killed during the war approaches half a million.[18] Estimated Russian recruitment levels fell below current casualty rates in April 2026. Additionally, having already had Telegram usage curtailed by the Kremlin, Russia's communication capabilities were further reduced on 1st February by SpaceX blocking Russian users of Starlink satellite communication.[19]

So what?

- Military analysts assess that the war remains 'competitive', with at least some of Ukraine's current advantage likely to be mitigated by future Russian innovations. Should Ukraine (supported by allies) be capable of holding Russia at a status of negligible territorial gains for a sufficient period, then Russia's strategy of eventually forcing a victory would be undermined. Negotiated peace may become more achievable.
- The above presented narrative represents a Western perspective and likely includes bias and intelligence gaps in Ukraine's favour. Regardless, countries supporting Ukraine can be expected to reinforce a narrative of a turning tide in Ukraine's favour for strategic gain (as heard in the Director of GCHQ's speech on 27th May); potentially including encouragement of the current US administration to maintain support for Ukraine and avoid reducing pressure on Russia.[20] Counter-narratives are anticipated, using influence operations and hybrid warfare tactics to undermine public support of governments most actively involved in supporting Ukraine and mitigating the wider Russian threat to Europe.
- Regardless of how or when the war between Russia and Ukraine ends, it is reasonable to infer that Russia will remain an unpredictable and real risk to European security, whilst the reliability of a NATO-dependent defence is uncertain. European countries continue to develop defensive alliances and initiatives in parallel, creating new areas of focus for cyber-enabled espionage, intelligence gathering, and disruption.[21,22]

26/05/2026

On 26th May, at a meeting of 'Quad' nations, Australia, India, Japan, and the US announced joint initiatives, including cooperation on critical minerals and energy security, and plans to develop maritime infrastructure in Fiji.[23] The Quad-funded port in Fiji is anticipated to be a commercial port, an area of infrastructure which China has previously offered to fund and support the development of.[24]

So what?

- The Quad's announcement highlights the reality that Fiji and other Pacific Islands have become a contested area of influence between China and Western nations - predominantly Australia and the US. This geopolitical trend is driven by two key factors: 1) The potential for military conflict with China over Taiwan, territory in the South China Sea, or other geopolitical themes has become more established as a threat requiring active preparation. Locations like the Pacific Islands are geographically well suited for regional defence or projecting military power. 2) The recent global disruptions caused by military conflict in the Strait of Hormuz highlight the benefits of diversifying shipping route infrastructure away from potential maritime chokepoints or port infrastructure over which rival nations hold significant control.
- For China, the Quad project represents a formal demonstration of regional neighbours seeking to reverse prior gains made by China, supported by the US. The specific project denies China the opportunity to develop specific commercial infrastructure between Asia and South America and creates new infrastructure which seeks to undermine China's dominance of critical mineral supply chains. Fijian government organisations, Quad partners, and global organisations involved in delivering and operating this project are at high risk of long-term compromise for intelligence gathering, similar to those reported by Samoa in February 2025, attributed to Chinese nation-state threat actor APT40.[25]
- Other Pacific islands (and organisations with regional operational footprints) will be monitoring the situation carefully. China has condemned the Quad's initiative and pushed back against allegations that it is seeking (or needs) to establish a location from which to setup a military base within the Pacific as a 'false narrative', and has also demonstrated its capabilities to conduct military attacks within international waters of the Pacific Ocean without a staging post.[26,27,28] Whilst it is assessed that China is unlikely to disrupt the Quad project or retaliate against Fijian interests overtly, disruptive or reputationally damaging attacks on Fijian public sector organisations or private sector activities supporting the Fijian economy may experience a period of heightened risk of 'criminal' or 'opportunistic' attacks. For Palau – an ally of Taiwan – prominent attacks by Dragonforce and Qilin in 2024 and 2025 coincided with the extension of relations with the US.[29,30]

Section 5

Emerging cyber security trend: Kitana, an AI-built Adversary-in-the-Middle managed fraud platform

In March's Threat Pulse, NCC Group highlighted the growing weaponisation of AI by threat actors ranging from organised crime groups to advanced persistent threats. While use cases vary, the primary risk remains consistent. AI enables attackers to scale operations, enhance capabilities, and accelerate tradecraft development.

Kitana is a prime example of this shift. Identified by NCC Group in April 2026, Kitana is a purpose-built Adversary-in-the-Middle (AiTM) fraud platform combining a transparent reverse proxy, real-time operator control, and Telegram-based command and control to enable interactive exploitation of e-commerce users.

Unlike traditional web skimming operations such as Magecart, which rely on compromised merchant environments, Kitana routes victims through attacker-controlled proxy domains that dynamically mirror legitimate sites, allowing real-time monitoring and intervention rather than passive data collection.[31]

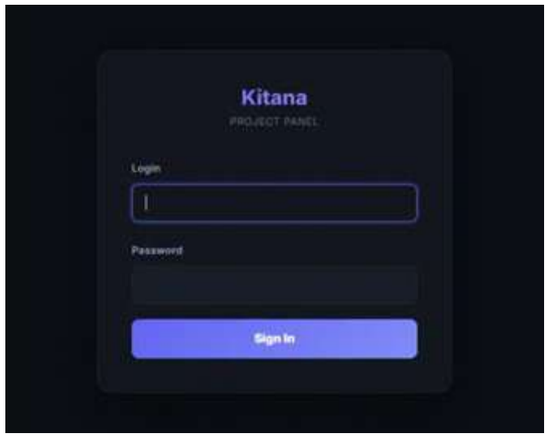


Figure 5: Kitana login panel

Observed infrastructure indicates targeting of hospitality sites in Canada and the United States, alongside e-commerce sites in Chile and Saudi Arabia, with the source code suggesting broader applicability.

Analysis of the exposed infrastructure shows that the platform is under active development, with experimentation using AI-assisted tooling. However, analysis of the source code reveals operational weaknesses, including hardcoded credentials and embedded API keys. These issues indicate insecure development practices and are consistent with rapid or insufficiently reviewed implementation, potentially associated with AI-assisted workflows.

Discovery

Kitana was identified during analysis of infrastructure previously linked to a supply chain compromise. A "Kitana Project Panel" login page was observed on the same host at a later stage, leading to the identification of 28 additional IP addresses exposing the same pages.

A publicly accessible directory was also identified containing Kitana's full source code. Although this directory was later removed, the infrastructure remains active. File timestamps dated 29th March 2026, and recent certificate registrations indicate recent development and deployment activity.

Platform architecture and attack flow

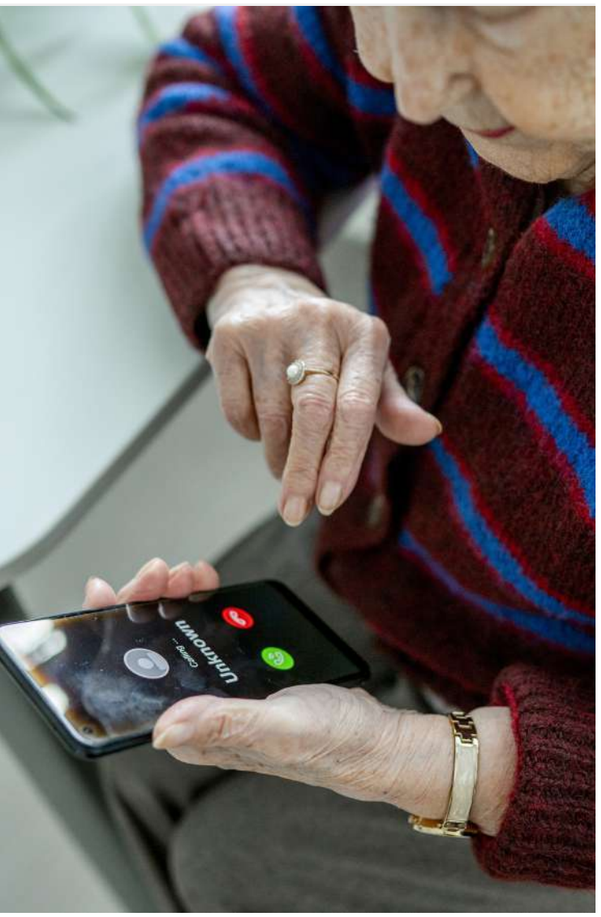
Kitana operates as a modular AiTM platform combining a reverse proxy, phishing infrastructure, web skimming capability, and real-time operator control. A Node.js reverse proxy mirrors target websites while a Python FastAPI backend manages session orchestration and data capture. Operators interact via a web panel and Telegram, enabling real-time control across sessions.

Victims are routed to the infrastructure via typosquatted domains and malicious advertising.

The incoming traffic is filtered through a Palladium traffic direction system, which evaluates requests based on IP reputation, geolocation, and browser characteristics to ensure only intended victims receive malicious content, while researchers and automated scanners are redirected to benign AI-generated decoy pages.

Users who pass filtering are served real-time mirrored sites on typosquatted domains, with all content rewritten in transit to preserve functionality while maintaining attacker control. During initial interaction, the victim's browser is fingerprinted using device, browser, and hardware attributes, which are linked to a session identifier to support profiling and targeting.

To evade detection, each session is assigned a synthetic IP address injected into request headers, while upstream traffic rotates across multiple User-Agent strings. Security headers such as CSP, HSTS, and X-Frame-Options are removed, and third-party resources are proxied through attacker infrastructure to avoid detection anomalies.



At the payment stage, the legitimate Bambora payment SDK is replaced with a cloned implementation that replicates validation logic but captures and exfiltrates full payment and personal data. A concurrent BIN lookup retrieves bank information used to generate realistic authentication prompts. Although Bambora was targeted in this instance, the platform supports substitution of alternative payment SDKs.

A defining feature of Kitana is its operator-driven model. A persistent Server-Sent Events connection allows operators to issue real-time commands, triggering overlays that mimic legitimate authentication workflows such as 3DS prompts and login requests. Commands enable progressive escalation, allowing extraction of authentication codes, credentials, and additional payment data within a single session.

Captured data is relayed via Telegram, allowing operators to respond in real time through an integrated interface. Session persistence is maintained through heartbeat messaging, while the panel aggregates session data and interaction history to support sustained exploitation.

Indicators of a maturing threat ecosystem

Kitana reflects the evolution of fraud tooling towards platformed, operator-driven ecosystems. Its modular architecture and multi-campaign capability align with broader Phishing-as-a-Service models, enabling scalable deployment across regions and targets.

The platform also demonstrates the expansion of real-time, interactive fraud. While AiTM techniques have been widely observed in enterprise phishing, their application to consumer payment fraud represents a shift towards more dynamic exploitation, where attackers actively control authentication flows during live sessions.

Additionally, Kitana incorporates monetisation-aware targeting through BIN-level intelligence, allowing operators to prioritise cards less likely to trigger authentication challenges. This reflects a trend towards more high value, outcome-driven fraud operations that are focused on maximising efficiency and return.

AI-assisted development

Kitana's source code contains multiple indicators consistent with AI-assisted development. Documentation and configuration files are structured in a machine-oriented format, including clearly segmented context blocks and explicitly defined logic flows, aligning with how large language models are typically prompted to generate or modify code.

In addition, the codebase exhibits a high degree of stylistic consistency across otherwise independent modules, including uniform structure, exhaustive branching logic, and repetitive implementation patterns that are characteristic of AI-generated output.

At the same time, the presence of basic security flaws, including hardcoded credentials and exposed API keys, indicates a lack of secure development practices. This combination of structured, highly regular code alongside fundamental implementation weaknesses suggests an emphasis on rapid development and functionality over secure engineering, - a pattern commonly associated with AI-assisted workflows where output is generated quickly but lacks rigorous validation.

The broader implication is that AI is reducing the technical and time investment required to develop complex, multi-component fraud platforms. Capabilities that previously required sustained expertise in web development, infrastructure management, and fraud operations can now be assembled more rapidly, lowering barriers to entry and accelerating the industrialisation of cybercrime.

```
# ═══════════════════════════════════════════════════════════
#  AUTODEPLOY: Reverse Proxy + Kitana + White Page + Cloaker
#  Usage: bash deploy.sh
#  Features: Luhn, OTP min 4 digits, address fallback,
#            hide cash/debit buttons, IPv6 fix, Google Maps proxy,
#            PHP-FPM with IP headers, footer links disabled
# ═══════════════════════════════════════════════════════════

RED='\033[0;31m'
GREEN='\033[0;32m'
YELLOW='\033[1;33m'
CYAN='\033[0;36m'
NC='\033[0m'

echo -e "${CYAN}"
echo "═══════════════════════════════════════════════"
echo "  AUTODEPLOY — Reverse Proxy + Kitana v2"
echo "═══════════════════════════════════════════════"
echo -e "${NC}"
```

Figure 6: Evidence of AI use in development

Recommendations

Kitana's ability to preserve legitimate site behaviour limits client-side detection, making infrastructure-level controls critical. For e-commerce organisations, monitoring typosquatted domains and registering high-risk lookalike domains is essential. Certificate transparency monitoring and threat intelligence can help identify malicious infrastructure early.

Improving customer awareness, particularly around domain verification and unexpected authentication prompts, remains an important secondary control in reducing the effectiveness of these attacks.


Under cyber attack?
Call our 24/7
Incident Response Hotline now.
NCC Group:
+44 (0)161 209 5200
response@nccgroup.com
www.nccgroup.com
Fox-IT:
+31 (0)88 369 23 78
fox@fox-it.com
www.fox-it.com
ncc group
FOX IT
part of ncc group