LOGICALIS
Architects of Change

Cyber Threat Intelligence in action

Protecting the Logicalis brand from cryptocurrency fraud

Detecting and disrupting brand impersonation before it escalates

As cyber threats evolve, attackers are increasingly targeting brand reputation and trust rather than systems and infrastructure. High-profile organisations are attractive targets, with brand credibility exploited to legitimise fraudulent schemes.

Logicalis recently detected and disrupted a brand impersonation campaign linked to a fraudulent cryptocurrency initiative. Through proactive Cyber Threat Intelligence (CTI), the threat was identified early and neutralised rapidly — preventing reputational and financial impact.

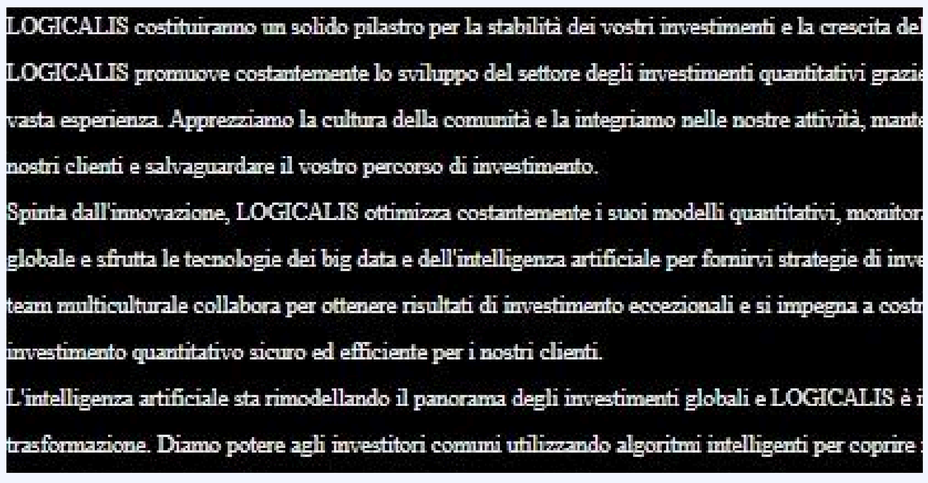
Brand impersonation attack

Brand impersonation attacks are difficult to detect because they typically operate outside the traditional security perimeter. In this case, there were no phishing emails, system compromises or internal alerts. The activity existed entirely on external websites and messaging platforms.

Without early detection, such attacks can result in serious reputational damage, legal exposure and loss of trust, even when no internal systems are breached.

How the threat emerged

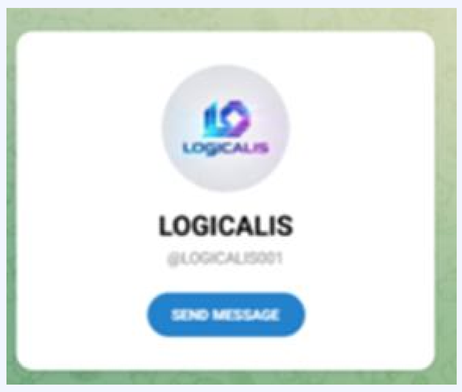
During routine monitoring, Logicalis' CTI capability identified the word "Logicalis" embedded within the HTML code of a suspicious external website.



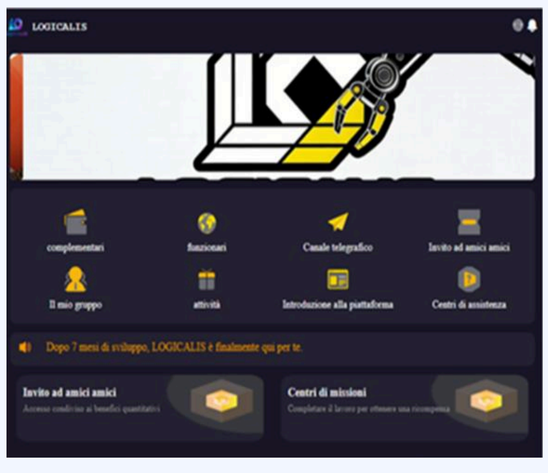
At that stage, this single indicator did not justify immediate takedown action. Instead, it was flagged, tracked and monitored by the CTI team.
Over time, attacker activity escalated:

- A fraudulent website was created using the Logicalis name and visual identity
- Fake social and messaging-channel presences appeared, including Telegram
- The campaign promoted a cryptocurrency investment designed to appear credible

This escalation confirmed clear malicious intent, that this was — an attempt to exploit Logicalis' brand reputation to deceive potential victims.



Attackers created a fraudulent Telegram presence using the Logicalis name and branding to promote a fake cryptocurrency campaign



Fraudulent platform leveraging the Logicalis brand: A fake cryptocurrency website designed to appear legitimate by using the Logicalis name and messaging to mislead users.

Decripto.org referencing the unauthorised use of the Logicalis brand in a cryptocurrency scam — underscoring the potential reputational impact of such attacks.

Solution: Cyber Threat Intelligence

Logicalis' Cyber Threat Intelligence (CTI) service was already operational when the threat surfaced, enabling rapid action as indicators accumulated.

CTI applies a "shift-left" approach to security, identifying threats during the preparation stage of the attack lifecycle, long before damage occurs.

In this case, the CTI team:

- Correlated indicators across domains, web content and social platforms
- Confirmed brand abuse and attacker intent
- Activated coordinated takedown playbooks across multiple attack vectors

By leveraging trusted relationships with digital platforms and infrastructure providers, the team was able to quickly remove fraudulent domains, disrupt supporting infrastructure, and pursue takedown actions across more challenging environments such as messaging platforms.

What could have become a high-impact brand incident was contained within hours, with the wider campaign dismantled in less than one day.

Outcomes and results

Early detection and rapid response delivered tangible business benefits beyond security alone:

Risk reduction

Swift action against external brand abuse before it translated into reputational or operational impact

Rapid containment

Marketing, PR, HR and Security teams were able to respond calmly and consistently, avoiding crisis management

Brand protection

Prevented public association between Logicalis and fraudulent cryptocurrency activity

Reduced organisational impact

Coordinated take-down actions were completed in under 24 hours

Demonstrated value

Swift action against external brand abuse before it translated into reputational or operational impact

Without CTI, this campaign could have run undetected for weeks or months, with reputational damage only becoming visible once harm had already occurred.

> “We are not waiting for the fraud to happen and then reacting.
>
> We are detecting the attack upfront — and that’s where the real value of Cyber Threat Intelligence is.”

Artur Martins
Cybersecurity Strategy Executive Advisor, Logicalis

Why proactive threat intelligence matters

Brand impersonation attacks rarely begin with obvious warning signs. They evolve quietly, often beyond the view of traditional security controls.

This incident demonstrates the importance of:

- Continuous external monitoring
- Attacker-centric intelligence
- Experienced human analysis

CTI does not wait for damage to occur.

By detecting weak signals, tracking escalation, and acting decisively at the right moment, Logicalis was able to protect its brand — turning a potential crisis into a quiet success.

Protecting your brand with Cyber Threat Intelligence

Logicalis delivers Cyber Threat Intelligence as a service, helping organisations identify emerging threats, detect brand abuse, and understand attacker behaviour before incidents escalate.

By monitoring the external threat landscape and acting early, CTI enables organisations to protect their brand reputation, customers, and business operations — not just their infrastructure..

→ Click here to learn more about Logicalis Cyber Threat Intelligence